Departamento de Informática

PROYECTO FIN DE CARRERA

Redes Sociales. Uso responsable y Controles

Autor: Anatolio Garrosa Fernandes
Tutor: Miguel Ángel Ramos

Leganés, Octubre 2015

Título: Redes Sociales. Uso responsable y controles
Autor: Anatolio Garrosa Fernandes
Director: Miguel Ángel Ramos

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

En primer lugar quiero agradecer a D. Miguel Ángel Ramos por acceder a ser mi tutor en este Proyecto, ya que durante estos años pensé que nunca lo presentaría. Gracias a su completa disposición y a sus consejos.

En segundo lugar a mi mujer Yolanda, a mis padres y hermanas, por sufrir constantemente conmigo y brindarme siempre todo su apoyo y cariño.

Por último, al que ha sido el impulsor de todo, mi pequeño Adrián. A ti porque desde que naciste pusiste mi vida patas arriba y a la vez la pusiste en orden.

Resumen

En este proyecto de fin de carrera se van a analizar los riesgos derivados del uso de las Redes Sociales, así como los inherentes al manejo de la información dentro de las mismas, entendiendo que estos riesgos hacen referencia a amenazas que vulneran los derechos de los usuarios relativos al manejo y uso de los datos de carácter personal y, en relación a estas amenazas, establecer medidas correctoras que minimicen (o eviten en su totalidad) el impacto de mismas.

Además se hará especial hincapié en las amenazas que pudieran afectar a los menores, atendiendo al especial riesgo e indefensión de este sector poblacional aportando así mismo recomendaciones para que padres y tutores puedan evitar un uso incorrecto de las redes sociales por parte de los menores anticipando de este modo situaciones de riesgo.

Igualmente, se planteará una alternativa para los proveedores de servicios de las redes sociales online en lo referente a la correcta gestión de la seguridad de la información dentro de su organización: la norma ISO 27001.

Palabras clave:

- Redes sociales online
- Medios sociales
- Datos personales
- Privacidad de la información
- Riesgos
- Consejos
- Menores

Abstract

In this final degree project is intended to analyze the risks related to social network management, as well as the ones inherent to data management into them, understanding that mentioned risks are referred to threats that violate user personal data management rights, and according to those threats to establish corrective actions to minimize (or even totally alleviate) their impact.

Also, more emphasis will be put on threats affecting children as this social group is considered to have special risk as they are helpless to them. Also we will provide some suggestions to parents and legal guardians in order to avoid a wrong use of Social Networks by children.

Also, there will be an alternative for service providers of online social networks referred to the proper management of information security within their organizations: ISO 27001 standard.

Keywords:

- Social Networks
- Social Media
- Personal Data
- Data Privacy
- Risks
- Suggestions
- Children

Índice general

Contenido

Índice de figuras

Índice de tablas

CAPÍTULO 1

INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

En este proyecto se hablará sobre las redes sociales online (RRSSO) y sobre los peligros derivados del uso de las mismas, refiriéndonos especialmente al tratamiento de información personal (y por tanto sensible), pero no circunscribiéndonos únicamente a ello.

Como se verá a lo largo de la exposición, las redes sociales online suponen una herramienta de comunicación fantástica que proporciona posibilidades hasta ahora desconocidas en la historia de la comunicación, desplazando a otras tales como el correo electrónico, el chat, o los clientes de mensajería instantánea (como el conocido Messenger).

La tremenda popularidad de la que gozan las redes sociales online hace que una parte considerable de la población las use de forma habitual, aunque no siempre lo haga con pleno conocimiento tanto de su funcionamiento como de los peligros que éstas entrañan.

En cuanto al modelo de crecimiento de las redes sociales online es conocido como piramidal (ahora se emplea el término "viral") es decir unos usuarios agregan o contactan con otros, que a su vez lo hacen con otros… resultando de este modo una "red" de personas (red social) interconectadas entre sí.

Podemos afirmar la globalidad de las RRSSO atendiendo a los datos de que se disponen acerca del uso de estos servicios. A este respecto cabe indicar que las cifras suelen diferir entre fuentes e informes, pero comparándolos, podríamos afirmar [1]:

- Cada año más de 2.000.000 millones de personas usan las redes sociales con regularidad.
- Más de 1.100 millones de usuarios emplean ***Facebook*** en todo el mundo, lo que la hace la red social más utilizada del mundo.

- ***YouTube*** tiene unos 1000 millones de usuarios que cada día pueden subir videos, verlos y comentarlos (incluso *streaming* y contenido disponible previo pago).
- ***Twitter*** tiene alrededor de 500 millones de usuarios, que disponen de 140 caracteres para realizar todo tipo de comentarios en la que es una de las redes con mayor viralidad.
- Cifra algo inferior de usuarios tiene ***Google+*** (unos 300 millones), muy utilizada para crear eventos y círculos entre las personas**.** Es parecida a ***Facebook*** pero, a pesar de ser de Google, no ha logrado conseguir el éxito que tiene su más directa competidora.
- ***LinkedIn*** es la RSO más empleada por profesionales. Tiene en torno a 260 millones de usuarios distribuidos en más de 1.5 millones de grupos.
- ***WhatsApp*** tiene alrededor de 600 millones de usuarios y aunque oficialmente se trata de un servicio de mensajería, comparte muchas de las características de las redes sociales online.

Tan sólo en España, el 82% de los internautas entre 18 y 55 años se declara como usuario de las redes sociales online, lo que supone en torno a 14 millones de usuarios. [2]

Todos estos datos nos aproximan a una idea del número total de usuarios que hacen uso de las redes sociales y de la cantidad de información relativa a éstos que circula diariamente por las mismas, así como del potencial riesgo que existe ante una actividad tan intensa ya sea este por parte de ataques malintencionados o por un uso indebido de las mencionadas redes.

1.2 Objetivos

El principal objetivo que se persigue con este proyecto es elaborar una serie de recomendaciones para los usuarios de las redes sociales online para que puedan hacer uso adecuado de las mismas y disfrutarlas en plenamente, evitando así situaciones peligrosas y desagradables.

Así mismo se persigue la adopción de un estándar por los proveedores de servicios de las redes sociales para reducir los riesgos de las mismas.

Para su consecución, se plantean otra serie de objetivos como son:

- Conocer qué son las redes sociales online y el porqué de su crecimiento.
- Poner en conocimiento de los usuarios sus derechos en relación al uso y manejo de redes sociales, así como las leyes que los sustentan.
- Identificar las amenazas existentes dentro de las redes sociales y los riesgos que de ellas se derivan.

1.3 Fases del desarrollo

Este proyecto de fin de carrera se ha ejecutado en varias fases, a saber:

- Una primera fase que ha consistido en la recopilación de la información aquí contenida, su preparación y clasificación.
- Una segunda, en la que se ha analizado la información recopilada, se ha clasificado y se ha ordenado para poder exponerla.

- Por último, se han elaborado la lista de recomendaciones y la checklist para procesos de auditoría que suponen el objetivo último del proyecto.

1.4 Medios empleados

Para este proyecto se ha requerido de un ordenador personal, así como de una conexión a internet, un editor de texto y un navegador de internet.

En cuanto a las fuentes consultadas, tal y como se puede ver en el apartado "Referencias" han sido de toda índole, principalmente el Boletín Oficial del Estado (BOE) y la página web de la Agencia Española de Protección de Datos, así como las versiones online de los principales periódicos nacionales y algunas publicaciones especializadas en tecnologías de la información y la comunicación (TIC), entre las que se incluyen las páginas web de INCIBE (antes INTECO) e ISACA.

Así mismo se ha requerido de la norma ISO/IEC 27001 para su estudio y comprensión.

1.5 Estructura de la memoria

Para facilitar la lectura de la memoria, se incluye a continuación un breve resumen del contenido de cada capítulo:

Capítulo 1: Introducción

En este capítulo se hace la presentación general del documento, el asunto que se pretende abordar y los objetivos que se persiguen.

Capítulo 2: Situación actual

En este capítulo se define que es una red social online y se recoge la situación actual de las mismas.

También se hace un breve repaso a su historia, y se muestran las clasificaciones más frecuentemente empleadas de las redes sociales.

Finalmente, se analiza el futuro de las redes sociales.

Capítulo 3: Aspectos legales y normativa aplicable

En este capítulo se recoge la normativa aplicable al tema que se desarrolla en el proyecto, ya sea esta internacional, europea o española.

Capítulo 4: Derechos, delitos, peligros y amenazas de las redes sociales

En este capítulo se recogen los derechos de las personas relativos al uso de redes sociales online, así como los delitos más frecuentes que surgen por su vulneración.

Se identificarán además los peligros y amenazas que del uso de las redes sociales derivan.

Capítulo 5: Recomendaciones y Consejos.

En este capítulo se recogen una serie de recomendaciones para los usuarios de redes sociales online con el fin de evitar los riesgos derivados de su uso, haciendo especial hincapié en aquellos que serán útiles a padres y tutores para asegurar un uso correcto por parte de los menores de este tipo de aplicaciones.

Así mismo, se recoge una alternativa propuesta para los suministradores de servicios de las redes sociales online: la aplicación de la norma ISO 27001.

Capítulo 6: Conclusiones y Futuras líneas de trabajo.

En este capítulo se recogen tanto las conclusiones generales del proyecto como las líneas futuras de investigación del tema tratado.

Capítulo 7: Planificación y Presupuesto

En este capítulo se recogen tanto la planificación de la elaboración del proyecto mediante un diagrama de Gantt como el presupuesto final del mismo atendiendo a los costes de los materiales empleados y de la persona que lo ha elaborado.

Capítulo 8: Glosario

En este capítulo se recogen y describen los términos empleados a lo largo del documento.

Capítulo 9: Anexos

En este capítulo se recogen algunas referencias de interés que permiten ampliar lo expuesto en el documento pero que se han considerado de vinculación más débil con el tema expuesto y que no se ha considerado incluir en el texto principal del mismo.

Capítulo 10: Referencias

En este capítulo se hace mención a la documentación que ha servido de base para la elaboración de este proyecto.

CAPÍTULO 2

SITUACIÓN ACTUAL

En primer lugar, cabe señalar que una red social no es sino un tipo específico de red, es decir: <<**Un ente formado por nodos que se interrelacionan formando conexiones y verifica la posición, centralidad e importancia de cada actor dentro de la red**>>.

Ahora bien, hay diversos tipos de redes dependo del objetivo de las mismas, es decir, dependiendo del bien o servicio que en ellas se intercambia (o, atendiendo a la definición previa, de la interrelación que se produce entre los diversos nodos).

Sin entrar en más detalle diremos que hay multitud de redes (telefonía, transportes…) y que nosotros examinaremos unas en concreto, las redes sociales online (en adelante RRSSO).

2.1 ¿Qué es una red social?

Lo primero que haremos será hacer una aproximación al término red social, que podría definirse del siguiente modo:

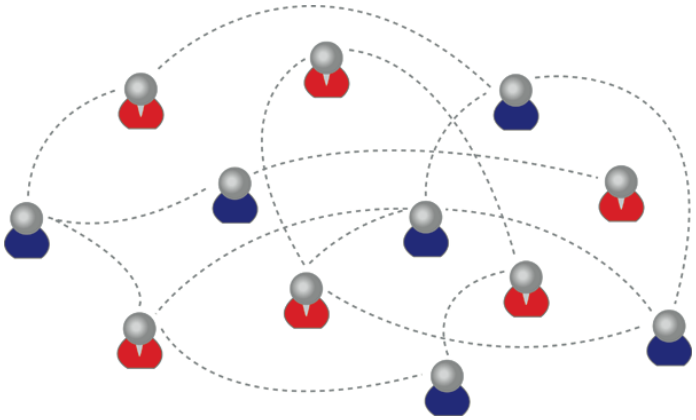
<<Una red social es una forma de representar una estructura social, asignándole un grafo, de modo que si dos elementos del conjunto de actores (tales como individuos u organizaciones) están relacionados de acuerdo a algún criterio (relación profesional, amistad, parentesco, etc.) entonces se construye una línea que conecta los nodos que representan a dichos elementos. El tipo de conexión representable en una red social es una relación diádica o lazo interpersonal>>. [3]

Fig.1 - Representación gráfica de una red social online

Otra posible definición, quizá menos académica, pero más intuitiva al respecto de lo que nos referimos es:

<<Una red social online se puede definir como una estructura virtual que genera relaciones entre las personas que la forman y sus contactos promoviendo la colaboración y el uso compartido de información>>. [4]

Fig.2 - Representación gráfica de una red social online



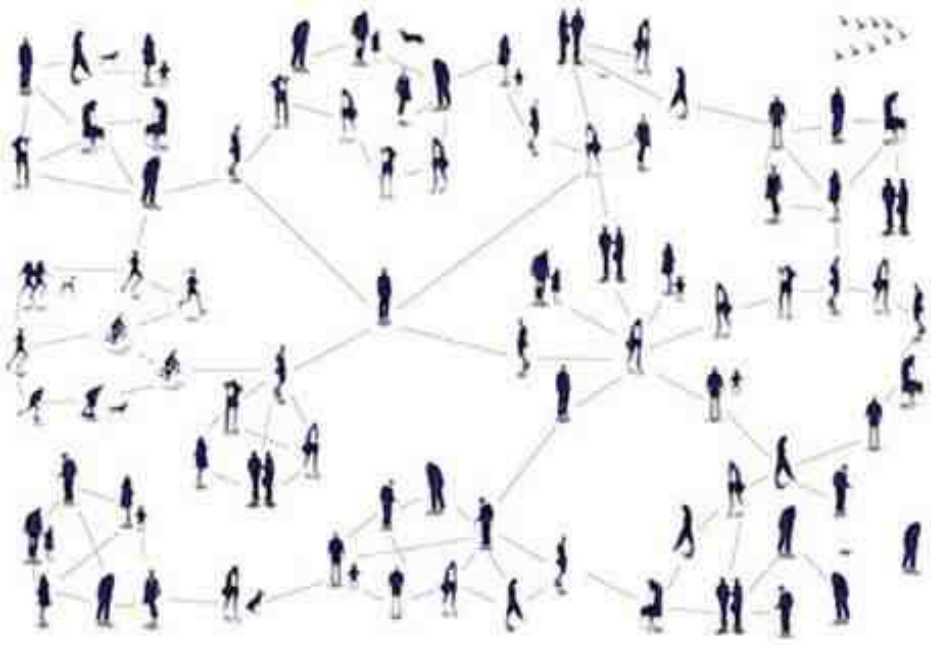
El concepto de red social online está fundamentado en la **teoría de los seis grados de separación** propuesta en 1929 por Frigyes Karinthy (y recogida

posteriormente en la obra "**Six Degrees: The Science of a Connected Age**" del sociólogo Duncan Watts), según la cual, cualquier individuo puede estar conectado a cualquier otro del planeta a través de una cadena de conocidos con no más de cinco intermediarios.

Aunque a priori esta idea pudiera parecer algo descabellada, hay que tener en cuenta que la mayor parte de estos grados, eslabones o contactos son los que se denomina un "vínculo latente", es decir, son desconocedores de este tipo de relación.

Según esta idea, bastan unos pocos eslabones de esta cadena para que el crecimiento geométrico de contactos permita conectar a dos personas cualesquiera a nivel mundial. [5].

Fig.3 - Representación gráfica de la teoría de los 6 grados de separación de Frigyes Karinthy



2.2 ¿Cómo funcionan las redes sociales online?

Las RRSSO establecen comunidades de Internet interconectadas en torno a un sitio web, que permiten establecer algún tipo de relaciones interpersonales.

El funcionamiento general de las RRSSO y de los sitios web que las sustentan es relativamente sencillo:

En primer lugar el usuario se crea una **cuenta de acceso** registrándose en la web, creando inmediatamente un **perfil personal** asociado a la misma en el que incluirá datos personales para poder ser identificado.

Con posterioridad el usuario creará su **red de contactos** (amigos, conocidos), enviándoles solicitudes de contacto (a veces llamadas de amistad, según la red) siendo de este modo incluido en la red de contactos del receptor de la solicitud.

Este proceso será repetido por todos los usuarios del sitio web, creando de este modo la red social.

Los perfiles de cada usuario pueden contener casi cualquier tipo de dato, que les permitirá tener una definición propia dentro de la red social:

- Nombre
- Edad
- Sexo
- Lugar de residencia
- Lugar de trabajo
- Lugares donde se ha estudiado

- Aficiones
- Preferencias políticas
- Fotografía…

Una de las particularidades de estos datos es que normalmente no son comprobados, es decir, podemos incluir algunos que no sean reales (aunque normalmente está prohibido según los términos de uso que imponen los administradores de los sitios web para el registro de la cuenta).

Esta particularidad, como se verá más adelante puede plantear no pocos problemas.

Las posibilidades de este tipo de redes son enormes, ya que usuarios (personas) que no se conocían con anterioridad, pueden llegar a entablar algún tipo de relación a través de personas comunes en sus propias redes particulares de contactos, incluso creando grupos de usuarios por aficiones o cualquier otro tipo de inclinaciones.

2.3 Historia de las redes sociales online

Veamos ahora una breve historia de las redes sociales online (en adelante RRSSO).

Aunque su origen es algo difuso, y dado que, como se verá más adelante, las relaciones humanas siempre tienden a establecerse en modo de redes sociales, el origen de las redes sociales online está inevitablemente ligado a la aparición de Internet, e incluso puede localizarse con anterioridad, pues los primeros intentos de comunicación entre ordenadores conectados en redes (aunque algo precarias, pero redes, al fin y al cabo) datan de los años 60, cuando surgieron como una iniciativa de los EEUU para establecer una red de comunicación militar (lo que posteriormente supondría el origen de Internet).

En lo tocante a las RRSSO tal y como las entendemos actualmente, se puede estimar su origen en 1995 cuando ***The Globe*** permite a usuarios la publicación de sus propios contenidos y conectar con otras personas con los mismos intereses y ***Randy Conrads*** crea la web ***Classmates*** que se ideó para que sus usuarios pudieran recuperar o mantener el contacto con sus antiguos amigos del colegio, universidad o distintos ámbitos laborales. En ella puede observarse el germen de otras redes posteriores como Facebook, que surgirán como punto de encuentro de alumnos y exalumnos.

Entre los años 1997 y 2000 surgieron diversos portales que permitían la creación de lo que se dio en llamar "Círculos de Amigos", tales como ***Six Degrees*** (1997), que ya permitía la creación de perfiles personales y duró hasta el año 2000, ***AsianAve*** (1997) o ***MiGente*** (2000) orientadas estas dos últimas a grupos étnicos (asiáticos y latinos respectivamente).

Hay algunos otros intentos de implantación de RRSSO de menor difusión que surgieron al calor de la oportunidad de negocio que estas incipientes redes brindaban tales como ***Friendster, Tribe*** o ***Xing***, pero no es hasta 2003 cuando surgen dos de las más potentes: ***MySpace*** y ***LinkedIn***.

MySpace brindaba multitud de posibilidades nuevas hasta ese momento como son la personalización de perfiles de usuario, grupos de interés, generación de blogs, compartición de videos, fotos y música, además de una herramienta de mensajería para la comunicación entre los usuarios, siendo la red más usada desde ese momento y hasta 2008.

LinkedIn por su parte ha llegado en plenitud de forma a nuestros días, con más de 240 millones de usuarios, y siendo aceptada como la red social líder dentro de la industria profesional.

En 2003, un estudiante de la Universidad de Harvard, ***Mark Zuckerberg***, crea ***Facemash*** en la que reunían varios datos de estudiantes de Harvard (entre ellos

fotografías), que habían sido extraídos sin autorización del sistema informático de Harvard sin permiso, por lo que fue sancionado y Facemash cancelado.

Al año siguiente, en 2004, los hermanos *Winklevoss* y *Divya Narendra*, también estudiantes de Hardvard, contactan con Zuckerberg para elaborar un proyecto en que estaban trabajando consistente en aunar en un directorio online los datos de fraternidades de la universidad que se encontraban dispersos en anuarios (o *facebooks* en inglés, de ahí su nombre posterior).

El 4 de Febrero del 2004, aparece el portal ***thefacebook***, y surge una disputa con los hermanos Winklevoss y con Narendra dado que consideraban que thefacebook se trataba de un plagio del portal en que tanto ellos como Zuckerberg trabajaban conjuntamente, ***HarvardConnection.com***. El nombre de thefacebook, pasaría a ser finalmente sustituido por ***Facebook***.

Con posterioridad Facebook amplió su uso para incluir a alumnos de secundaria y otras instituciones educativas y, finalmente se amplió a cualquier usuario con la única restricción de que tuviera un correo electrónico para efectuar el alta de la cuenta (2006).

En 2006 se crea ***Tuenti***, una red social generalista española, así como ***Twitter*** que surge como un servicio de *microblogging* a través de *tweets* o mensajes cortos (140 caracteres) que sus usuarios pueden enviar desde su sitio web, mediante un SMS o desde otras aplicacione*s (Twinkle, Twidroid, Tweetie).* [6]

Entre los años 2007 y 2008 se lanzan versiones de Facebook en otros idiomas como el español, traducido por voluntarios y que permitió su expansión en España y en toda Latinoamérica.

En 2010 Google lanza ***Google Buzz*** integrada en su gestor de correo Gmail, y aparece Pinterest, que al año siguiente (2011) ya habría alcanzado los 10 millones de visitas mensuales, mientras Google apuesta por ***Google +***, una red generalista que intentará competir con Facebook en adelante.

Hay que tener en cuenta que las cifras relativas a las RRSSO quedan anticuadas en cuestión de meses y que nuevas plataformas aparecen continuamente aprovechando la expansión viral de las redes sociales.

El crecimiento de las redes sociales online sólo puede ser analizado desde el nuevo paradigma comunicativo que supuso el cambio en el modo de entender la comunicación Web, pasando de las antiguas páginas web estáticas, que aportaban información, pero limitaban enormemente la posibilidad de recibir *feedback*, apenas mediante algunos comentarios y cuya finalidad era consumir contenidos (lo que se conoce como ***Web 1.0***), a una auténtica ***Web Social*** o ***Web 2.0*** donde la comunicación fluye en tiempo real e interrelaciona a los sujetos de un modo cambiante y dinámico mediante el uso de un canal abierto, que puede tener diversos objetivos de forma simultánea (multidireccional), en el que se comparten, no sólo información, sino también ideas y experiencias, permitiendo una participación mucho más colaborativa por parte de los diversos actores en el intercambio de información con el resto.

La ***Web 2.0*** no es más que la evolución de la Web o Internet en el que los usuarios dejan de ser usuarios pasivos para convertirse en usuarios activos, que participan y contribuyen en el contenido de la red siendo capaces de dar soporte y formar parte de una sociedad que se informa, comunica y genera conocimiento. [7]

Las redes sociales generan un *espacio virtual* en el que el usuario cuenta con unos datos personales con los que se construye un perfil público (o al menos relativamente) con algún tipo de información obligatoria, y con alguna otra que le parezca apropiada (gustos, intereses, aficiones…), y con el que podrá interactuar con el resto de usuarios de la red.

Por ejemplo personas que hayan estudiado en el mismo colegio o universidad, que residan o hayan residido en la misma localidad, o también, mediante la creación de *grupos*, personas que compartan inquietudes, motivaciones, aficiones o problemas.

Esta posibilidad de agrupar usuarios, por características comunes de los perfiles, propicia la aparición espontánea de *actos comunicativos* (interacciones entre los

usuarios actores), que van desde el simple intercambio de comentarios u opiniones a otras con mayor entidad (foros, eventos…), pudiendo llegar a establecerse lazos personales más o menos estables (de amistad, amorosos, profesionales…).

2.4 Tipos de redes sociales

Las redes sociales pueden clasificarse de múltiples modos, pero nosotros haremos la primera división atendiendo a la dimensión social de las mismas, por lo que las clasificaremos como sigue:

- **Redes sociales offline o analógicas**, que son las relaciones que el ser humano ha establecido de forma natural a lo largo de la historia (familia, amigos…) y que no conllevan la intermediación de un aparato o sistema electrónico.

- **Redes sociales digitales** (RSD), a través de medios electrónicos.

- **Redes sociales mixtas**, mezcla de los dos tipos anteriores.

Quisiera hacer una primera anotación al respecto y es que algunos autores no consideran todas las redes digitales como redes online, ya que entienden que para eso deben estar montadas desde un sitio web propio que les da presencia en Internet.

Así, algunos no consideran a WhatsApp como una RSO, sino sólo como una RSD, aunque, debido a la gran cantidad de características que comparten, en este proyecto no haremos tal diferenciación.

Una vez hecho este inciso, pasaremos al estudio de las RRSSO.

Su tipología se ha planteado desde muchos puntos de vista (sobre si son gratuitas o de pago, por ejemplo), aunque la clasificación más empleada es la que lo hace atendiendo al grado de especialización de la RSO, diferenciando entre redes generalistas u horizontales y especializadas o verticales.

Redes sociales generalistas

También denominadas redes sociales horizontales, no versan sobre ningún tema en concreto y se dirigen hacia el gran público. La motivación de los usuarios al acceder a ellas es la interrelación general, sin un propósito concreto, por lo que no se centran en los temas sino en los usuarios.

Su función principal es la de poner en contacto a personas entre sí, por lo que las funciones básicas de estas redes son: la creación de usuarios, agregar contactos y compartir contenidos.

Algunas de ellas son:

- ***Facebook:***

  Es la red social más extendida, tanto en España como en el resto del mundo. Creada por Mark Zuckerberg, se desarrolló inicialmente como una red para estudiantes de la Universidad Harvard, pero posteriormente se habilitó para cualquier persona que quiera registrarse.

  Permite crear grupos, eventos, páginas, participar en juegos sociales e incluso se pueden crear aplicaciones para la misma.

- ***QQ:***

  Se trata de la red más utilizada en China, con más de 800 millones de usuarios. Creada en 1995 como un programa de mensajería, actualmente es mucho más que eso.

Permite enviar **e-mails** (QQMail), disponer de un **disco duro virtual** (Wangluo Yingpan), escribir un **blog** (QQZone), un **microblog** (Tencent Weibo), escuchar **música** (QQYinyue), **comprar online** (Paipai) y **jugar en red** (QQYouxi).

- ***Hi5:***

Se fundó en 2003 por *Ramu Yalamanchi* y está enfocada al público más joven por su evolución, desde 2010 a un sitio centrado en juegos sociales. Fue vendida a su competidor *Tagged* en 2011 aunque sigue operativa.

Es una de las redes sociales más extendidas en Latinoamérica, con más de 300 millones de usuarios.

- ***MySpace:***

Lanzada en 2003 es propiedad de propiedad de Specific Media LLC y la estrella de pop *Justin Timberlake*.

Fue la RSO más visitada del mundo de 2003 a 2008 aunque desde entonces su número de usuarios ha ido decreciendo de forma constante. Permite personalizar los perfiles de los usuarios mediante códigos HTML en algunas áreas así como incluir videos y contenido en flash.

Es muy utilizada por grupos musicales para compartir sus creaciones, que pueden inscribirse para promover y vender su música. No importa si el artista ya es famoso o no; artistas y aspirantes pueden cargar sus canciones para el MySpace y tener acceso a millones de personas en sólo día.

En 2008 se lanzó *MySpace Music*, competidor de *iTunes* para servicio de descarga de música.

Este es un caso de una red, generalista en sus orígenes, pero que ha sobrevivido gracias a la especialización.

- ***Google+:***

Red social propiedad de Google fue puesta en funcionamiento en 2011 para usuarios mayores de 13 años.

Nació como competidor de Facebook y cuenta con 2.200 millones de perfiles creados pero en realidad **sólo un 9% de ellos han escrito alguna vez algo en la red social**. El número incluye personas que usan su perfil de Google+ para comentar en vídeos de YouTube, la acción más común. Google se ha escudado en el pasado apuntando que las interacciones privadas, que generalmente no se reflejan en estos números, son una parte importante de la red social que no puede ser medida.

Las últimas acciones de Google+ parecen indicar que da la batalla por perdida y que Google+ acabará desapareciendo. A partir de ahora para ver las fotos de Google+ no será necesario pasar por la propia red social, algo que parece que indica que las diversas funciones de Google van a ser separadas pero ya veremos si para ser desarrolladas e impulsadas por separado o para ser vendidas al mejor postor. [8]

- ***Tuenti:***

Red social española dirigida a la población joven. Se denomina a sí misma como una plataforma social de comunicación. Esta compañía española, inaugurada en noviembre de 2006, llegó a contar con más de 13 millones de usuarios, pero hoy sus cifras son bien distintas. A parte de las posibilidades comunes, dispone de Tuenti Sitios, Tuenti Páginas y Tuenti Juegos.

Esta red, que era la más utilizada entre los menores de 25 años de nuestro país, ha perdido frente al empuje de otras como Twitter o Facebook, tanto que la compañía parece haber dado de lado la red social, apostando por una nueva línea de negocio consistente en la creación de una Operadora Móvil Virtual (OMV), que ya cuenta con más de 300.000 clientes. [9].

- ***Netlog:***

  Esta es la historia de otro fracaso.

  Destinada a la juventud europea y latinoamericana llegó a tener más de 87 millones de usuarios registrados en 2010 en 25 idiomas diferentes.

  El 30 de Septiembre del año pasado Netlog anunció su cierre remitiendo un correo a sus usuarios para que, si lo deseaban, procedieran a la descarga de toda la información que habían aportado.

- ***Badoo:***

  Fundada en 2006, tuvo gran repercusión en los medios de comunicación por su crecimiento y perspectivas de futuro. Actualmente opera en más de 150 países.

  Un estudio realizado en 2009 sobre la protección de la privacidad en 45 redes sociales situó a Badoo en una de las últimas posiciones.

  Actualmente es usada por unos 200 millones de personas en el mundo.

Redes sociales especializadas

También son denominadas redes sociales verticales.

Dentro de las redes sociales hay una marcada tendencia hacia la especialización. Aunque las redes sociales más generalistas ganan diariamente miles de usuarios, otras tantas especializadas se crean para dar cabida a los gustos e intereses de las personas que buscan un espacio de intercambio común. De hecho, el número de

redes sociales especializadas de nueva creación es mucho mayor que el de las generalistas.

Hay sitios que permiten al usuario crear sus propias redes sociales de forma rápida, y mediante unos pasos sencillos. Las opciones que existen actualmente ofrecen una alta funcionalidad sin necesidad de conocimientos expertos. Se pueden compartir datos mediante su propio servicio de almacenamiento en línea, y relacionarnos con las personas que consideremos en un entorno cerrado y a salvo de intromisiones o posibles fugas, lo que permite crear redes sociales de cualquier tipo, tantos como se desee.

Por temática:

- ***Profesionales***.

  Las redes profesionales se dirigen principalmente a los negocios y actividades comerciales. Permiten compartir experiencias o crear grupos, asociando a empresas y usuarios que estén interesados en una colaboración laboral. Los usuarios de estas redes poseen un perfil profesional, en el que incluyen su ocupación actual o su currículo académico y laboral, entre otros requisitos. Ejemplos de este tipo son *LinkedIn*, *Xing* o *Viadeo*.

  Cabe indicar que incluso hay redes ultraespecializadas como *HR.com*, orientada a los profesionales de recursos humanos, o *ResearchGate* y *Epernicus*, destinadas a investigadores científicos.

  Hay que tener en consideración que las empresas utilizan cada día más este tipo de redes para la contratación de nuevos profesionales.

- ***Aficiones***.

  Estas RRSSO se dirigen a aficionados de cualquier disciplina o hobby, motivo por el que las hay muy variadas: *BallHype* es una red social para amantes

de todo tipo de deportes, *Bottletalk* lo es para amantes de la enología**,** *Fotolog* o *Flickr* para amantes de la fotografía, *Motortopia* para aficionados al mundo del motor, *MyDogSpace* para amantes de los perros o *Goodreads* y *Shelfari* para amantes de los libros. [10].

- ***Sociales***.

  Surgen en torno a preocupaciones sociales como la ecología, la igualdad social o la sostenibilidad, tal es el caso de *WiserEarth*, *SocialVibe*, *Care2* o *Posibl.com*.

- ***Viajes***.

  Son redes que conectan viajeros de cualquier lugar para compartir experiencias tales como *WAYN*, *TrayBuddy*, *Travellerspoint*, *Minube* o *Exploroo*, que permiten planificar viajes y vacaciones sin necesidad de las tradicionales guías de viaje.

- ***Identidad cultural***.

  En los últimos años, debido al poder de la globalización, se aprecia un incremento de referencia al origen por parte de muchos grupos que crean sus propias redes para mantener la identidad. Ejemplos de esto son: *Spaniards*, la comunidad de españoles en el mundo; y *Asianave*, una red social para los asiático-americanos.

- ***Otras temáticas.***

  Encontramos, por ejemplo, redes sociales especializadas en el aprendizaje de idiomas, como *Busuu*; plataformas para talentos artísticos, como *Taltopia*; o sobre compras, como *Shoomo*.

Por actividad:

- ***Microblogging***.

  Estas redes sociales ofrecen un servicio de envío y publicación de mensajes breves de texto. También permiten seguir a otros usuarios, aunque esto no establece necesariamente una relación recíproca, como los seguidores o *followers* de los famosos en *Twitter*. Dentro de esta categoría están: *Twitter*, *Plurk*, *Muugoo* o *Tumblr*, entre otras.

- ***Juegos***.

  En estas plataformas se congregan usuarios para jugar y relacionarse con otras personas mediante los servicios que ofrecen. A pesar de que muchos creen que son, simplemente, sitios web de juegos virtuales, las redes sociales que se crean en torno a ellos establecen interacciones tan potentes que, incluso, muchos expertos de las ciencias sociales han estudiado el comportamiento de los colectivos y usuarios dentro de ellos. Algunas son: *Friendster*, *Foursquare*, *Second Life*, *Haboo*, *Wipley*, *Nosplay*, *Lineage* o la más conocida, *World Of Warcraft*.

- ***Geolocalización***.

  También llamadas de georreferencia, estas RRSSO permiten mostrar el posicionamiento con el que se define la localización de un objeto, ya sea una persona, un monumento o un restaurante. Mediante ellas, los usuarios pueden localizar el contenido digital que comparten. Ejemplos de este tipo son: *Foursquare*, *Metaki*, *Ipoki* y *Panoramio*.

- ***Marcadores sociales***.

  La actividad principal de los usuarios de marcadores sociales es almacenar y clasificar enlaces para ser compartidos con otros y, así mismo, conocer sus listas de recursos. Estos servicios ofrecen la posibilidad de comentar

y votar los contenidos de los miembros, enviar mensajes y crear grupos. Los más populares son: *Delicious*, *Digg* y *Diigo*.

- ***Compartir objetos***.

  Dentro de estas redes sus miembros comparten contenidos diversos como vídeos, fotografías o noticias, y mediante esta colaboración se establecen las relaciones que tampoco tienen que ser mutuas de forma obligatoria, al igual que se ha indicado para el caso de microbbloging.

Por contenido compartido:

- ***Fotografías***.

  Estos servicios ofrecen la posibilidad de almacenar, ordenar, buscar y compartir fotografías. Las más importantes en número de usuarios son: *Flickr*, *Fotolog*, *Pinterest* y *Panoramio*.

- ***Música***.

  Especializadas en escuchar, clasificar y compartir música, permiten crear listas de contactos y conocer, en tiempo real, las preferencias musicales de otros miembros. Ejemplos de este tipo son las redes: *Last.fm*, *Blip.fm* o *Groovershark*.

- ***Vídeos***.

  Los sitios web de almacenamiento de vídeos se han popularizado de tal manera que en los últimos años incorporan la creación de perfiles y listas de amigos para la participación colectiva mediante los recursos de los usuarios, y los gustos sobre los mismos. Algunas de estas redes son *Youtube*, *Vimeo*, *Dailymotion*, *Pinterest* y *Flickr*.

- ***Documentos***.

  Son redes que se usan para localizar, publicar y compartir aquellos textos que se ajusten a nuestras preferencias de una manera fácil y accesible. Su mayor exponente es *Scribd*.

- ***Presentaciones***.

  Al igual que ocurre con los documentos, el trabajo colaborativo y la participación marcan estas redes sociales que ofrecen a los usuarios la posibilidad de clasificar, y compartir sus presentaciones profesionales, personales o académicas. Las más conocidas son: *SlideShare* y *Slideboom.*

- ***Noticias***.

  Los servicios centrados en compartir noticias y actualizaciones, generalmente, son agregadores en tiempo real que permiten al usuario ver en un único sitio la información que más le interesa, y mediante ella relacionarse estableciendo hilos de conversación con otros miembros. Algunos de ellos son: *Menéame, Auatu, Digg* y *Friendfeed*.

- ***Lectura***.

  Estas redes sociales no sólo comparten opiniones sobre libros o lecturas, sino que además pueden clasificar sus preferencias literarias y crear una biblioteca virtual de referencias. Ejemplos de esta categoría son: *Anobii*, *Librarything, Entrelectores, WeRead* y *Wattpad*. [11]

2.5 Características comunes

Aunque los diversos tipos mencionados de redes sociales difieren en ciertos aspectos, también comparten algunos de ellos de modo generalizado. A continuación pasamos a describirlos:

- Fomentan la difusión viral de la red social, a través de cada uno de los usuarios que la componen, empleando este método como principal forma de crecimiento del número de usuarios.

- Tienen como finalidad principal poner en contacto a usuarios (personas), de tal forma que a través de la plataforma electrónica se facilite la conexión de forma sencilla y rápida.

- Permiten la interacción entre todos los usuarios de la plataforma, ya sea compartiendo información, contactando o facilitando contactos de interés para el otro usuario. [12]

2.6 Situación actual de las redes sociales.

Según un estudio de la ***Online Business School*** que analiza las tendencias de uso de las redes sociales en España y otros países, España cuenta con una población online de 23 millones de personas, lo que supone casi la mitad de la población total del país.

El estudio indica que el 73% de ellos, es decir, casi 17 millones de usuarios utiliza las RRSSO de forma mensual en 2014, y únicamente el 8% dice no utilizar red alguna.

En cuando al medio de acceso, más un 73% dice acceder a las redes sociales desde cualquier dispositivo que lo permita indistintamente, un 68% desde ordenador, un 46% lo desde el teléfono móvil (Smartphone) y un 21% dice que lo hace empleando una Tableta.

Las redes sociales más usadas en el 2014 por los internautas españoles son ***Facebook, Google+*** **y** ***Twitter***. El 88% de los españoles que utilizan Internet tiene cuenta en ***Facebook***, que experimenta un 1% de subida con respecto al año anterior, el 59% en ***Google+*** (3% de mejora respecto a 2013) y el 56% en ***Twitter*** (que mejora en un 2%).

La principal red profesional es ***Linkedin***, usada por un 32% de los internautas nacionalesl. ***Instagram*** **y** ***Pinterest*** son las redes que más crecen entre los usuarios españoles, con un 25% y 19% de usuarios españoles de redes sociales respectivamente. [13]

En la siguiente tabla se recogen las principales redes sociales del mundo ordenadas por el número de usuarios que las usan.

Tabla 1 – Redes sociales con mayor número de usuarios en el mundo

1	Facebook	**Número de usuarios:** 1.100 millones Esta red social sigue liderando **el primer puesto** siendo la que más usuarios registrados tiene de todas las demás **redes sociales**
2	YouTube	**Número de usuarios:** 1.000 millones ¿Quién no ha visto alguna vez un vídeo en **YouTube?** Incluso hay quien gana dinero subiendo sus propios videos, ya que reciben un incentivo económico por cada 1000 visitas. Son los conocidos como *Youtubers*.

3	QQ	**Número de usuarios:** 815 millones Ésta es la **red social más usada** de **China** y la tercera con más usuarios en el mundo. Es muy completa: equivale a Messenger, Facebook y Twitter juntos, además de poder escribir un blog con ella o enviar emails.
4	Qzone	**Número de usuarios:** 620 millones Otra red social de origen chino que triunfa por **agrupar actividades** como escribir un blog, alojar fotos y música, y un chat de mensajería instantánea que aloja a más de **50 millones** de usuarios cada día.
5	WeChat	**Número de usuarios:** 600 millones Este servicio de **mensajería instantánea** es uno de los principales competidores de la app WhatsApp. Su origen es chino y ya hay más de **40 millones de usuarios** que lo utilizan fuera del país asiático.
6	Twitter	**Número de usuarios:** 500 millones Aunque esta red social **tiene muchos seguidores**, también la limitación de tareas (y caracteres) que se pueden usar en ella hace que muchas personas prefieran crear cuentas en redes sociales con más funcionalidades.
7	WhatsApp	**Número de usuarios:** 400 millones Fue una de las pioneras en permitir la **mensajería instantánea** en los teléfonos móviles sin ningún coste (excepto el de tu tarifa de datos o WiFi), aunque hace os años (Marzo 2013) implantó una cuota anual algo inferior a 1€.
8	Sina Weibo	**Número de usuarios:** 400 millones Esta red social china es el **equivalente a Twitter** aunque últimamente incluye también funciones similares a Facebook

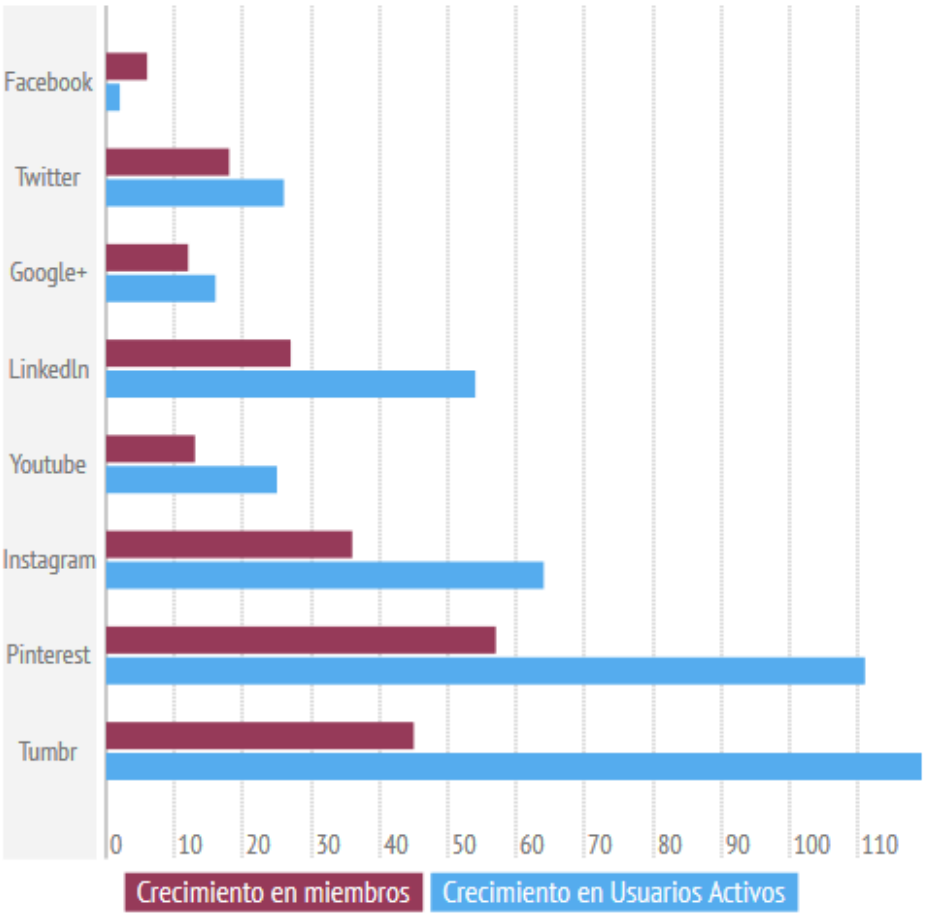
9	Hi5	**Número de usuarios:** 330 millones Esta es una de las redes sociales más populares en Amércia Latina y países como India y Tailandia. Su modelo es bastante parecido a **Facebook** y también tiene un gran número de usuarios en EEUU.
10	Tagged	**Número de usuarios:** 330 millones Esta red social es muy similar a Facebook y **MySpace** en cuanto a funcionamiento. Los creadores de Tagged la diseñaron con la finalidad de que las personas **conociesen a otros** en periodos breves de tiempo.

Esto da idea de la gran variedad de redes sociales que existen, y de lo especializadas o específicas que pueden llegar a ser por su temática o distribución sociocultural.

Hay que tener en cuenta, que esto es una foto estática, pero que el estado de las redes sociales online cambia día a día tanto en lo que a número de usuarios se refiere como en las redes disponibles.

Se muestra a continuación un gráfico de Febrero de 2015 en el que se recoge el crecimiento tanto en número absoluto de usuarios como de usuarios activos experimentado por algunas de las redes sociales más relevantes desde Septiembre de 2014 hasta el citado mes [14]:

Fig.4 - Incremento de usuarios en redes sociales 09/14 – 02/15



Así, redes como *Google+*, *Tuenti* o *Fotolog*, que en su momento gozaron de cierta popularidad parecen haber caído en el olvido de los internautas que se decantan por nuevas opciones.

Por ejemplo, en el caso concreto de la red *Tuenti*, parece que la principal causa de la pérdida de cuentas ha sido la adopción por parte de los usuarios españoles de *Facebook* como red social generalista.

2.7 El futuro de las redes sociales online

Sin duda, las redes sociales buscarán un cambio de estrategia para adaptarse a las costumbres de los usuarios siendo más específicas en sus fórmulas y funciones adaptándose al estilo de vida o el comportamiento de cada usuario

Si relacionábamos el auge de las redes sociales online con la aparición de la Web 2.0, inevitablemente hay que relacionar el futuro de las redes sociales con la incipiente Web 3.0, una nueva vuelta de tuerca en la evolución de la web que trata de avanzar en lo relativo a los contenidos, convirtiéndola en una *red semántica:*

Mientras la Web 2.0 está gestionada por el propio usuario, la Web 3.0 está orientada hacia el protagonismo de motores informáticos y procesadores de información que entienden de lógica descriptiva en diversos lenguajes más elaborados de metadatos, utilizando software avanzado como el RDF/XML o el SPARQL y que se gestiona mediante el *cloud computing* (en la nube), con mayor grado de viralidad incluso que la Web 2.0, y cuya finalidad es que los motores de búsqueda y las máquinas encargadas nos puedan brindar la información que necesitamos "a la carta" basándose en nuestros perfiles de la Red, y en el rastro de nuestra actividad que dejamos en la red. [15]

De este modo, llegamos al concepto *de Social Media* (Medios de Comunicación sociales), que refieren tanto a la estrategia como a las herramientas empleadas en las Redes Sociales Online para la difusión de información, así como de contenidos con fines publicitarios y/o comerciales. [16]

También se han usado otros términos para referirse a los medios de comunicación social «*como contenido generado por el usuario*» o «*medios de comunicación generados por el consumidor*».

Una de las múltiples oportunidades comerciales que brindan las redes sociales es que se puede realizar un marketing ad-hoc para cada grupo de interés (incluso para cada usuario) pues se conocen sus intereses y opiniones y pueden realizarse campañas comerciales menos intrusivas de forma específica.

Los medios de comunicación social, están reemplazando lenta pero inexorablemente a los tradicionales medios de masas (*mass media*), debido a una serie de características que les son propias y que suponen una importante ventaja comunicativa. A saber:

- ***Audiencia:***

  Ambos medios emplean una tecnología tal que permiten a cualquier persona el acceso a los mismos, de modo que ambas pueden llegar a una audiencia global.

- ***Accesibilidad:***

  Los medios de masas son generalmente de pago y son propiedad de un particular o del gobierno, mientras que los medios sociales están en general disponibles para cualquier persona con poco o ningún coste.

- ***Facilidad de uso por los creadores:***

  En los medios industriales la producción del contenido requiere normalmente de recursos y conocimientos especializados. La mayoría de los medios sociales no, o en algunos casos se reinventa habilidades, de modo que cualquier persona puede ser un productor en estos medios.

- ***Facilidad de uso por los creadores:***

  En los medios industriales la producción del contenido requiere normalmente de recursos y conocimientos especializados. La mayoría de los medios sociales no, o en algunos casos se reinventa habilidades, de modo que cualquier persona puede ser un productor en estos medios.

- ***Instantaneidad:***

  El tiempo que transcurre entre la producción del contenido y su entrega a las audiencias puede ser largo (días, semanas o incluso meses) en comparación con los medios sociales (que puede ser capaz brindar contenido prácticamente de forma instantánea o sólo con muy pequeños retraso en su publicación. Los

medios Industriales están evolucionando con la adopción de recursos y tecnologías de modo que esta característica puede no ser la más distintiva en poco tiempo.

- ***Edición del contenido:***

  En los medios industriales, una vez creado el contenido éste no puede ser alterado (una vez que el artículo de una revista se ha impreso y distribuido los cambios no se pueden hacer en ese mismo artículo), mientras que los medios sociales no solo se enriquecen con los comentarios de las audiencias, sino que el contenido puede ser alterado instantáneamente por los productores, mejorando en contenido para las audiencias. [17]

Mientras que los medios de masas se pueden ver sujetos a determinada línea editorial, y deben responder ante propietarios y/o accionistas, los medios sociales no tienen esa condición por lo que frecuentemente pueden servir como herramienta de presión a gobiernos y poderes políticos en busca de trasparencia.

A este respecto, sirva a modo de ejemplo el caso de China, donde algunas de las redes sociales online más usadas del mundo están prohibidas y para las que se han generado otras sustitutivas propias:

- ***Youtube***, que se censuró en 2009, sustituida por ***Youku***.
- La red de microblogging más famosa del mundo, ***Twitter***, también fue prohibida en 2009, creándose ***Weibo***, para sustituirla.
- Desde el principio, el gobierno chino ha sido muy crítico con ***Facebook*** y ésta sufrió frecuentes bloqueos, hasta que en Mayo de 2011, fue sustituida por ***Renren***, con más de 40 millones de usuarios a día de hoy.
- A finales del 2012, China anunciaba el bloqueo de ***Skype***. Desde el gobierno chino, se informó que solamente ***China Telecom*** y ***China Unicom*** podrían proveer servicios VoIP como lo hace *Skype*. Ambas compañías son controladas por el estado.
- ***Foursquare***, vetada en el 4 de Junio 2010 debido a que muchas personas hicieron *checkin* en la Plaza de Tiananmen en el 21 aniversario de la masacre de

Tiananmen. Los mensajes de protesta sobre este hecho histórico fue el detonante para que el gobierno bloqueara esta red.

- ***Flicker***, bloqueado el mismo día 4 de junio pero del 2009. Justo 20 años después de las protestas en la Plaza Tiananmen.
- ***Google+*,** que sufrió su bloqueo en su primer día de estreno. [18]

A modo de muestra, se aporta un titular del diario español *El Mundo* de 1 de Octubre del año pasado. [19]

El caso es que la falta de regulación y las características de las redes sociales que ya hemos mencionado con anterioridad (viralidad, interacción entre usuarios, interconexión, anonimato…), las convierten no sólo en un arma por la lucha de los derechos sociales y por la transparencia, sino en arma de difusión para otros propósitos menos loables como son el terrorismo o el crimen organizado, algo que describiremos con más detalle en el apartado de Riesgos.

Se aportan ejemplos de noticias de medios de la prensa española a este respecto como muestra de lo expuesto [20]:


Qué!

Actualidad | España | Internacional | Economía | Tecnología | Deportes | Famosos | Curiosas | Ocio | Estilo de vida | Blogs | Más

Internacional

Buscar Fotos Vídeos

Las redes sociales amplifican la amenaza terrorista, según la CIA

El director de la Agencia Central de Inteligencia estadounidense (CIA), John Brennan, ha denunciado que las redes sociales y las nuevas tecnologías amplifican "enormemente" la amenaza global del terrorismo, al permitir la difusión de atentados y ataques de forma casi simultánea.

EP 13 de marzo de 2015

Además, hay una serie de usos o aplicaciones de las redes sociales en los ámbitos más cotidianos y diversos de nuestra vida diaria, que pasaremos a indicar a continuación.

Las redes sociales como medio divulgativo y de investigación:

Se define a las ***redes sociales educativas o de divulgación científica*** como grupos de personas relacionadas y conectadas por el interés común en la educación. La alta interrelación que brindan las redes sociales entre las personas y las herramientas que proporcionan desarrolla espacios comunes para investigadores, alumnos y profesores en lo que son entornos colaborativos de participación que permiten crear dinámicas formativas globales (dentro y fuera de las aulas), con un rápido flujo de información, desarrollando la socialización del conocimiento. En este sentido, alejarse de las redes sociales implica en gran parte aislamiento científico. [21]

Las redes sociales como medio de difusión política:

Los gobiernos y partidos políticos disponen ahora de nueva formas de llegar a los ciudadanos/electores, y pueden hacerlo de forma más ágil y en cualquier momento (no sólo en campaña electoral).

A su vez, los ciudadanos disponen ahora de un medio para ser escuchados, para generar y participar de corrientes de opinión, generando debates acerca esta o aquella cuestión.

En países donde hay mayor represión informativa, las redes sociales han demostrado ser una herramienta valiosa para la información y la denuncia (véase el caso ya expuesto de China).

Esta situación se trata de combatir mediante la censura de páginas o contenidos, como ya se ha indicado, mediante procedimientos de *blacklisting* o control de IPs entre otros.

Pero esta situación no sólo se limita a gobiernos represivos: En países occidentales también se han organizado manifestaciones desde las redes sociales, en ocasiones, por grupos ajenos a organización política alguna, que persiguen un fin común.

Tal es el caso de las iniciativas "Rodea el congreso", y las "Marchas por la dignidad" convocadas en España, así como otras contra la corrupción acaecidas en Mallorca o Barcelona. [22]

A este respecto, se aporta ejemplo de algún titular reciente:


LA CIUDAD · NUESTRA NOTICIA · PORTADA

Una manifestación convocada por las redes sociales provoca daños en varios edificios

20 de febrero de 2015 by Redacción No Comments

Desde el día 1 de Julio de 2015, este tipo de convocatorias se consideran ilegales dada la aprobación y entrada en vigor, tras su publicación en el BOE, de la reciente "Ley de Seguridad Ciudadana", que en su artículo 30.3 recoge:

<<A los efectos de esta ley se considerarán organizadores o promotores de las reuniones en lugares de tránsito público o manifestaciones las personas físicas o jurídicas que hayan suscrito la preceptiva comunicación. Asimismo, incluso no habiendo suscrito o presentado la comunicación, también se considerarán organizadores o promotores quienes de hecho las presidan, dirijan o ejerzan actos

semejantes, o quienes por publicaciones o declaraciones de convocatoria de las mismas, por las manifestaciones orales o escritas que en ellas se difundan, por los lemas, banderas u otros signos que ostenten o por cualesquiera otros hechos pueda determinarse razonablemente que son directores de aquellas>>. [23]

Por este motivo la ley ha sido dada en denominarse "Ley Mordaza" por parte de ciertos colectivos, tales como las agrupaciones de internautas, que defienden que difundir por las redes una convocatoria de manifestación no les hace responsables de la misma (y por tanto responsables de los daños que en ella se ocasionen o de los altercados que en la misma pudieran producirse)..

Así mismo, las RRSSO pueden ser usadas con otros fines políticos como son la celebración de mítines, campus u otro tipo de actos políticos, así como para la creación de grupos de simpatizantes, para la difusión de noticias (lo que habitualmente se denomina "globo sonda" para determinar el impacto en la población de la adopción de alguna medida o norma)…

Las redes sociales como medio de difusión informativa:

Si nos referimos a las noticias, como aquella información relevante que históricamente se nos ha brindado en los medios de comunicación clásicos (prensa, radio y televisión), las RRSSO son las protagonistas absolutas en cuanto a distribución de las noticias se refiere.

Según un estudio de la *CNN*, más del 40% de los usuarios comparten las noticias mediante las redes sociales. *Facebook*, *Twitter* o *YouTube* son los canales más populares para llevar a cabo esta actividad, seguidos del correo electrónico, el SMS y los mensajes instantáneos. El mismo estudio indica que el 27% de los que comparten la información difunden el 87% de las noticias recientes. De media, los miembros del estudio recibían más de 26 noticias por semana en las redes sociales.

Además, se recoge en el estudio que las noticias más compartidas son aquellas que más impactantes visualmente, las de deportes, las de ciencia y tecnología, economía y de interés humano. [24]

Las redes sociales como medio de difusión publicitaria:

Las empresas tienen en las redes sociales un medio de difusión de sus productos y servicios que no requiere de costosas campañas de marketing. Es lo que se conoce **como *Marketing 2.0***.

Mientras que el Marketing 1.0 se centraba en el producto, el 2.0 lo hace en el cliente. La evolución para el Marketing 2.0 con el surgimiento y auge de las redes sociales supone un paso más allá en lo que a comunicación con el cliente, motivo por el cual algunos autores hablan ya del marketing 3.0.

Como hemos dicho, ahora las campañas se centran no el producto, sino en el público objetivo al que van dirigidas. Este público es un activo valioso para la marca, ya que tiene opinión, conoce el producto de primera mano y tiene una red de contactos con la que compartir esa información, creando una reputación online del producto.

Existe un decálogo que recoge los principios en los que se fundamenta este nuevo marketing:

1. Ama a tus consumidores y respeta a tus competidores.
2. Sé sensible al cambio, prepárate para la transformación.
3. Protege tu marca, sé claro acerca de quién eres.
4. Los consumidores son diversos, dirígete primero a aquellos que se pueden beneficiar más de ti.
5. Ofrece siempre un buen producto a un precio justo.
6. Sé accesible siempre y ofrece noticias de calidad.
7. Consigue a tus clientes, mantenlos y hazlos crecer.
8. No importa de qué sea tu negocio, siempre será un negocio de servicio.
9. Diferénciate siempre en términos de calidad, costo y tiempo de entrega.
10. Archiva información relevante y usa tu sabiduría al tomar una decisión.[25]

El 23% de los usuarios españoles de **redes sociales** siguió activamente a sus **marcas** preferidas en 2014, y el 33% usa las *Fan Pages* de las marcas como **Centro de Atención**, según estudio de la *Online Business School (OBS)*.

Según dicho estudio, un 56% de estos usuarios siguen a una marca principalmente para obtener una recompensa, ya sea en forma de regalo o descuento; un 41% lo hacen por la calidad de los productos de la marca, y un 33% lo hacen por la calidad de los Servicios de Atención al Cliente vía redes sociales. [26]

Como se ha podido ver, las redes sociales tienen usos y aplicaciones diversas en la mayoría de los ámbitos relacionados con el día a día de las personas: educación, información (económica, deportiva), política, compras, y obviamente, las ya mencionadas en apartados previos, como son búsqueda de empleo, compartir aficiones o simplemente relacionarnos con nuestros contactos, familiares y amigos.

Es por todo este conjunto por lo que se habla de un cambio de paradigma, y es la causa de que los Medios Sociales presenten unas expectativas de futuro alentadoras, más allá de la propia situación individual de cada red social, que puede pasar de un éxito absoluto al fracaso más rotundo en cuestión de pocos meses tal y como hemos comentado.

CAPÍTULO 3

ASPECTOS LEGALES Y NORMATIVA APLICABLE

La gran implantación y el crecimiento viral de las redes sociales online entre toda clase de públicos, ha generado una situación en la cual los datos personales de una persona pueden hacerse accesibles desde casi cualquier parte del mundo y en tiempo real, lo que puede suponer un grave problema en lo tocante a la privacidad de los datos personales de los usuarios de las RRSSO.

Es importante reseñar, que en la relación entre los proveedores de servicios propietarios de los portales online que dan soporte a las diversas plataformas o redes sociales online y los usuarios, la parte más débil siempre son estos últimos.

Grosso modo, podríamos indicar que (casi todas) las redes sociales online se componen de:

Software: que conforma los portales y las operaciones de la red social.

Hardware: los servidores, discos y otros dispositivos donde se alojan el software y los datos.

Datos personales: los relativos a los perfiles de usuarios.

Otra información: comentarios, fotos, videos…

Pues bien, la información contenida en los datos arriba indicados la aporta libre y voluntariamente el usuario, y este es uno de los datos más importantes a tener en cuenta, dado que facilitamos la información nosotros mismos.

Paremos un momento y recordemos un acontecimiento verídico que ocurrió hace algunos años (2003) en Madrid en el cual se localizaron numerosos currículum vitae de solicitantes de empleo de una conocida cadena de supermercados tirados en la basura y con diversas anotaciones (algunas de carácter racista) realizadas en los mismos. [27]

Ahora, pensemos en qué ocurriría si esa misma situación se reprodujese e una red social online.

Mientras que en el caso indicado, la repercusión era limitada por su alcance y difusión, en nuestro hipotético caso para las redes sociales online, la repercusión es casi

global e instantánea. En este caso, las mencionadas características de las redes sociales podrían convertir todas las ventajas de las RRSSO (fácil difusión de la información, acceso multiplataforma…) en un serio inconveniente.

Hay quien pudiera pensar "¿Dónde está el problema en la difusión de unos currículum vitae?". La respuesta bien pudiera ser que en los mismos se recogen datos de carácter personal, pero además, debido a la amplia clasificación de redes sociales online (véase capítulo previo) podríamos estar hablando de cualquier tipo de información personal, relativa a gustos, pareceres, experiencias, inclinaciones políticas…

Si pensamos de nuevo en un caso hipotético, podríamos encontrarnos en uno en el que alguno de los usuarios de estas redes sociales online esté efectuando una búsqueda activa de empleo. El sujeto ha preparado su currículum vitae y la entrevista de manera exhaustiva pero se ve rechazado debido a algún tipo de publicación que realizó hace algún tiempo en las redes sociales.

Este caso hipotético, no lo es tanto cuando la mayoría de los responsables de los departamentos de recursos humanos de grandes empresas indica que realiza contrataciones a través de redes sociales online (78%), y casi en su totalidad las emplean para la búsqueda de candidatos (94%).

De ellos, 47% indica que emplean las redes sociales para el descarte de los candidatos: El 83% descarta a los que consumen alcohol o drogas, el 51% a los que hacen algún tipo de mención explícita a la violencia, el 71% a los que aparecen en fotografías en posturas sexuales, el 65% a los que escriben con graves errores gramaticales… [28]

Es decir, que algo que se publica fuera del ámbito de la entrevista, puede servir para aportar información valiosa sobre el solicitante de empleo, información que sería muy costoso y complicado conseguir de cualquier otra manera.

No sólo se puede realizar un filtrado de candidatos mediante las redes sociales, también se conocen algunos casos de despidos por opiniones vertidas en redes sociales, como en el titular que se recoge a continuación. [29]


Redes sociales

Despedida por Twitter

Una estadounidense es despedida antes de su primer día en una pizzería por llamar "mierda" a su nuevo empleo

11.02.2015 | 04:36

Atendiendo a situaciones como las descritas, parece que como usuarios estamos descuidando la información que se difunde mediante las redes sociales (gran parte de ella de carácter personal) y que no estamos teniendo debidamente en cuenta quien puede recibir y hacer uso de dicha información.

3.1 Privacidad en las redes sociales online

En este punto debemos introducir un nuevo término, la ***Privacidad***, que según la RAE, se define como:

<<**Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión**>>.

Si acudimos a la ***Declaración Universal de los Derechos Humanos***, en ***su artículo 12*** se recoge expresamente:

<<**Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques**>>. [30]

De igual modo en la ***Constitución Española*** en su ***artículo 18*** también se hace mención expresa:

<<**Derecho al honor, a la propia imagen, y a la intimidad personal y familiar. Inviolabilidad del domicilio, salvo consentimiento del titular, resolución judicial o flagrante delito. Inviolabilidad de las comunicaciones**>>.

¿En qué manera encajan estos derechos dentro de un entorno de redes sociales online, Internet y comunicaciones electrónicas?

Para adecuar el término al nuevo paradigma de las comunicaciones hoy en día, podemos hacer referencia al término "Privacidad en Internet".

La ***privacidad en Internet*** se refiere al control de la información que posee un determinado usuario que se conecta a Internet, interactuando por medio de diversos servicios en línea con los que intercambia datos durante la navegación.

Hay que tener en cuenta que actualmente no existe una privacidad real en Internet, debido a que aún hay una estructura primitiva informática, aunque avanza y evoluciona cada día. [31]

Si nos referimos concretamente a las redes sociales online, podemos definir la privacidad como:

<<***Se entiende por privacidad en una red social online el nivel de protección de que disponen todos los datos e informaciones que una persona introduce en una red social, en cuanto al grado de accesibilidad a ellos que otros usuarios o internautas pueden tener***>>.[32]

La mayor parte de redes sociales online 2.0 nos permiten diversas opciones a través de las que podemos configurar la privacidad de nuestra cuenta. Así, como titulares de la misma, podemos **decidir qué queremos compartir con el resto de**

usuarios de la red social (o de Internet), además de la facultad de poder redefinir estos parámetros de seguridad en cualquier momento para establecer un nivel distinto de privacidad si fuera requerido.

En la mayor parte de las redes sociales online, se establece una primera diferenciación entre aquellos usuarios que disponen de una cuenta en la propia red social y aquellos que no (usuarios invitados). A su vez, dentro de aquellos que sí disponen de cuenta, suele hacerse una distinción entre los que forman parte de nuestra lista de contactos (amigos, familia, compañeros,….) y aquellos que carecen de vínculo alguno con nosotros.

Algunas redes sociales, como en el caso de *Facebook*, incluso permiten ajustar la privacidad de un modo más definido: podemos elegir no ser indexados por motores de búsqueda, como los empleados por buscadores internos o externos (como *Google* o *Yahoo!, por ejemplo*).

De aquí, pueden surgir dos problemas:

a) El primero, es que no nos molestemos en revisar las opciones de configuración de seguridad y/o privacidad en nuestra cuenta (esto incluye, entre otros, el uso de una contraseña segura), pues por todos es bien conocido el uso del "Siguiente, Siguiente, Aceptar…" empleado por una gran parte de los usuarios finales de productos informáticos (no solo de redes sociales online, aunque también de éstas).

b) El segundo problema, aunque escapa completa e irremediablemente al control del usuario final, hace referencia a la protección de los datos que los administradores de las diversas redes sociales profesan. Los usuarios, es decir, los verdaderos dueños de los datos, se encuentran en manos de la profesionalidad y buena praxis de los encargados de gestionar y custodiar dicha información.

Dicho lo cual, hay ciertos mecanismos que nos permiten evitar o reducir el impacto de posibles malas prácticas como veremos más adelante.

3.2 Legislación sobre la seguridad de los datos personales

Atendiendo a lo ya expuesto en el punto previo, profundizaremos un poco más en los aspectos jurídicos/legales a tener en cuenta, y que se hayan relacionados con la temática aquí expuesta, haciendo hincapié en el ya mencionado derecho a la Privacidad (o a la intimidad), y en el aún no mencionado derecho a la Propiedad Intelectual (e Industrial).

Trataremos de mencionar cronológicamente las normativas nacionales e internacionales aplicables al tratamiento de datos personales para, de este modo, ver en qué modo han ido evolucionando las leyes para adaptarse a la cambiante realidad social y tecnológica.

3.2.1 Legislación internacional

El punto de partida, como es lógico, es la Declaración universal de los Derechos Humanos aprobada en la ONU en 1948, tras la Segunda Guerra Mundial:

Declaración Universal de los Derechos Humanos

10 de Diciembre de 1948

Artículo 12.

Pacto Internacional de los Derechos Civiles y Políticos
16 de Diciembre de 1966

Artículo 17.

(Ambos comparten texto)

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. [33]

Debido a que en EEUU no existe una única legislación relativa al tratamiento de datos personales para la totalidad de sus estados miembros, el Departamento de Comercio de los EEUU presentó en 1999 a la Unión Europea (UE) un documento con la finalidad de discutir y consensuar un acuerdo que permitiese a los operadores de servicios de Internet allí ubicados la libre transferencia de datos entre la UE y los EEUU.

De ello surgió un borrador que contenía los siguientes 7 puntos descritos a continuación:

Acuerdo de Puerto Seguro
16 de Diciembre de 1999.

1. ***Notificación****:*

   Los individuos deben ser informados de que sus datos están siendo recogidos y sobre la forma en que se utilizarán.

2. ***Decisión****:*

Las personas deben tener la posibilidad de decidir acerca de la recogida y transferencia de los datos a terceros.

3. ***Transferencias sucesivas**:*

   Los datos solo pueden transferirse a otras organizaciones si éstas cumplen con principios de protección de datos adecuados.

4. ***Seguridad**:*

   Se deben hacer esfuerzos razonables para evitar la pérdida de la información recopilada.

5. ***Integridad de los datos**:*

   Los datos deben ser fiables y consecuentes con el propósito para el que fueron recopilados.

6. ***Acceso**:*

   Las personas deben ser capaces de acceder a la información y corregirla o eliminarla si no es exacta.

7. ***Cumplimiento**:*

   Se deberá disponer de medios efectivos para hacer valer estas reglas. [34]

A continuación se menciona cronológicamente la normativa de la UE al respecto.

3.2.2 Legislación europea

Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales

4 de Noviembre de 1950

Artículo 8.

1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*

2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*

3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*

4. *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. [35]*

Convenio para la protección de individuos con respecto al proceso automático de datos personales

28 de Enero de 1981

Artículo 5.

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

c) Se obtendrán y se tratarán leal y legítimamente.

d) Se registrarán para finalidades determinadas y legítimas y no se utilizarán de una forma incompatible con dichas finalidades.

e) Serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.

f) Serán exactos y si fuera necesario puestos al día.

g) Se conservarán bajo una forma que permita la identificación de las personas concernidas durante un periodo de tiempo que no exceda el necesario para las finalidades para las cuales se hayan registrado. [36]

En 1995 y fundamentado en gran parte en el anterior convenio de 1981, el Parlamento Europeo adopta la Directiva 95/46/CE que constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la UE. Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

Directiva 95/46/CE del Parlamento Europeo y del Consejo
24 de octubre de 1995

Artículo 6.

Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;
b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;
c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a

los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

e) *conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.*

Artículo 7.

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) *el interesado ha dado su consentimiento de forma inequívoca, o*
b) *es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o*
c) *es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o*
d) *es necesario para proteger el interés vital del interesado, o*
e) *es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o*
f) *es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.*

Artículo 8.

1. *Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.*
2. *Lo dispuesto en el apartado 1 no se aplicará cuando*

   a) *el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o*
   b) *el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o*
   c) *el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o*
   d) *el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o*
   e) *el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial [37]*

Carta de los Derechos Fundamentales de la Unión Europea

7 de Diciembre de 2000

(Proclamada versión adaptada el 12 de Diciembre de 2007 tras el Tratado de Lisboa)

Artículo 7.

Respeto de la vida privada y familiar.
Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8.

Protección de datos de carácter personal

1. *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.*
3. *El respeto de estas normas estará sujeto al control de una autoridad independiente.*

Directiva 2001/29/CE del Parlamento Europeo y del Consejo

22 de Mayo de 2001

En este caso se trata de una directiva que pretende homogeneizar dentro de los estados miembros de la UE las legislaciones en lo referente a los derechos de autor y de propiedad intelectual. Al tratarse de directrices que deben ser implementadas por normativas propias de los distintos estados miembros, pueden surgir diferencias en cuanto a la interpretación de las mismas y por tanto dar ligar a marcos legislativos bastante diferentes en los distintos estados.

Artículo 2.

Derecho de reproducción

Los Estados miembros establecerán el derecho exclusivo a autorizar o prohibir la reproducción directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de la totalidad o parte:

a) a los autores, de sus obras;
b) a los artistas, intérpretes o ejecutantes, de las fijaciones de sus actuaciones;
c) a los productores de fonogramas, de sus fonogramas;
d) a los productores de las primeras fijaciones de películas, del original y las copias de sus películas;
e) a los organismos de radiodifusión, de las fijaciones de sus emisiones, con independencia de que éstas se transmitan por procedimientos alámbricos o inalámbricos, inclusive por cable o satélite.

Artículo 3.

Derecho de comunicación al público de obras y derecho de poner a disposición del público prestaciones protegidas

1. *Los Estados miembros establecerán en favor de los autores el derecho exclusivo a autorizar o prohibir cualquier comunicación al público de sus obras, por procedimientos alámbricos o inalámbricos, incluida la puesta a disposición del público de sus obras de tal forma que cualquier persona pueda acceder a ellas desde el lugar y en el momento que elija.*
2. *Los Estados miembros concederán el derecho exclusivo a autorizar o prohibir la puesta a disposición del público, por procedimientos alámbricos o inalámbricos, de tal forma que cualquier persona pueda tener acceso a ellos desde el lugar y en el momento que elija:*

   a) a los artistas, intérpretes o ejecutantes, de las fijaciones de sus actuaciones;

b) a los productores de fonogramas, de sus fonogramas;

c) a los productores de las primeras fijaciones de películas, del original y las copias de sus películas;

d) a los organismos de radiodifusión, de las fijaciones de sus emisiones, con independencia de que éstas se transmitan por procedimientos alámbricos o inalámbricos, inclusive por cable o satélite.

3. Ningún acto de comunicación al público o de puesta a disposición del público con arreglo al presente artículo podrá dar lugar al agotamiento de los derechos a que se refieren los apartados 1 y 2.

Artículo 4.

Derecho de distribución

1. Los Estados miembros establecerán en favor de los autores, respecto del original de sus obras o copias de ellas, el derecho exclusivo de autorizar o prohibir toda forma de distribución al público, ya sea mediante venta o por cualquier otro medio.

2. El derecho de distribución respecto del original o de copias de las obras no se agotará en la Comunidad en tanto no sea realizada en ella la primera venta u otro tipo de cesión de la propiedad del objeto por el titular del derecho o con su consentimiento.

Artículo 5.

Excepciones y limitaciones

1. Los actos de reproducción provisional a que se refiere el artículo 2, que sean transitorios o accesorios y formen parte integrante y esencial de un proceso tecnológico y cuya única finalidad consista en facilitar:

a) una transmisión en una red entre terceras partes por un intermediario, o

b) una utilización lícita de una obra o prestación protegidas, y que no tengan por sí mismos una significación económica independiente, estarán exentos del derecho de reproducción contemplado en el artículo 2.

2. Los Estados miembros podrán establecer excepciones o limitaciones al derecho de reproducción contemplado en el artículo 2 en los siguientes casos:

a) en relación con reproducciones sobre papel u otro soporte similar en las que se utilice una técnica fotográfica de cualquier tipo u otro proceso con efectos similares, a excepción de las partituras, siempre que los titulares de los derechos reciban una compensación equitativa;
b) en relación con reproducciones en cualquier soporte efectuadas por una persona física para uso privado y sin fines directa o indirectamente comerciales, siempre que los titulares de los derechos reciban una compensación equitativa, teniendo en cuenta si se aplican o no a la obra o prestación de que se trate las medidas tecnológicas contempladas en el artículo 6;
c) en relación con actos específicos de reproducción efectuados por bibliotecas, centros de enseñanza o museos accesibles al público, o por archivos, que no tengan intención de obtener un beneficio económico o comercial directo o indirecto;
d) cuando se trate de grabaciones efímeras de obras, realizadas por organismos de radiodifusión por sus propios medios y para sus propias emisiones; podrá autorizarse la conservación de estas grabaciones en archivos oficiales, a causa de su carácter documental excepcional;
e) en relación con reproducciones de radiodifusiones efectuadas por instituciones sociales que no persigan fines comerciales, como hospitales o prisiones, a condición de que los titulares de los derechos reciban una compensación equitativa.

3. Los Estados miembros podrán establecer excepciones o limitaciones a los derechos a que se refieren los artículos 2 y 3 en los siguientes casos:

a) *cuando el uso tenga únicamente por objeto la ilustración con fines educativos o de investigación científica, siempre que, salvo en los casos en que resulte imposible, se indique la fuente, con inclusión del nombre del autor, y en la medida en que esté justificado por la finalidad no comercial perseguida;*

b) *cuando el uso se realice en beneficio de personas con minusvalías, guarde una relación directa con la minusvalía y no tenga un carácter comercial, en la medida en que lo exija la minusvalía considerada;*

c) *cuando la prensa reproduzca o se quiera comunicar o poner a disposición del público artículos publicados sobre temas de actualidad económica, política o religiosa, o emisiones de obras o prestaciones del mismo carácter, en los casos en que dicho uso no esté reservado de manera expresa, y siempre que se indique la fuente, incluido el nombre del autor, o bien cuando el uso de obras o prestaciones guarde conexión con la información sobre acontecimientos de actualidad, en la medida en que esté justificado por la finalidad informativa y siempre que, salvo en los casos en que resulte imposible, se indique la fuente, con inclusión del nombre del autor;*

d) *cuando se trate de citas con fines de crítica o reseña, siempre y cuando éstas se refieran a una obra o prestación que se haya puesto ya legalmente a disposición del público, se indique, salvo en los casos en que resulte imposible, la fuente, con inclusión del nombre del autor, y se haga buen uso de ellas, y en la medida en que lo exija el objetivo específico perseguido;*

e) *cuando el uso se realice con fines de seguridad pública o para garantizar el correcto desarrollo de procedimientos administrativos, parlamentarios o judiciales, o para asegurar una cobertura adecuada de dichos procedimientos;*

f) *cuando se trate de discursos políticos y de extractos de conferencias públicas u obras o prestaciones protegidas similares en la medida en que lo justifique la finalidad informativa y siempre que, salvo en los casos en que resulte imposible, se indique la fuente, con inclusión del nombre del autor;*

g) *cuando el uso se realice durante celebraciones religiosas o celebraciones oficiales organizadas por una autoridad pública;*

h) cuando se usen obras, tales como obras de arquitectura o escultura, realizadas para estar situadas de forma permanente en lugares públicos;

i) cuando se trate de una inclusión incidental de una obra o prestación en otro material;

j) cuando el uso tenga la finalidad de anunciar la exposición pública o la venta de obras de arte, en la medida en que resulte necesaria para promocionar el acto, con exclusión de cualquier otro uso comercial;

k) cuando el uso se realice a efectos de caricatura, parodia o pastiche;

l) cuando se use en relación con la demostración o reparación de equipos;

m) cuando se use una obra de arte en forma de edificio o dibujo o plano de un edificio con la intención de reconstruir dicho edificio;

n) cuando el uso consista en la comunicación a personas concretas del público o la puesta a su disposición, a efectos de investigación o de estudio personal, a través de terminales especializados instalados en los locales de los establecimientos mencionados en la letra c) del apartado 2, de obras y prestaciones que figuran en sus colecciones y que no son objeto de condiciones de adquisición o de licencia;

o) cuando el uso se realice en otros casos de importancia menor en que ya se prevean excepciones o limitaciones en el Derecho nacional, siempre se refieran únicamente a usos analógicos y que no afecten a la libre circulación de bienes y servicios en el interior de la Comunidad, sin perjuicio de las otras excepciones y limitaciones previstas en el presente artículo. [38]

Finalmente, y aunque no posee valor normativo, quiero mencionar la **Comunicación sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad** (02/05/2007) que realizó la Comisión del Parlamento Europeo, con la finalidad de defender los derechos e los ciudadanos europeos en materia de protección de datos mediante herramientas tecnológicas denominadas "**PET**".

Las "tecnologías de protección del derecho a la intimidad", en adelante PET, son sistemas tecnológicos destinados a reducir e incluso eliminar el impacto de las nuevas tecnologías de la información sobre los derechos de protección de datos e intimidad de los usuarios sin menoscabar las funcionalidades de los sistemas afectados.

Además, indicar que en la **Comunicación de la Comisión sobre el papel de la administración electrónica en el futuro de Europa**, se indica expresamente el uso de PET en la administración electrónica para generar la confianza necesaria en los usuarios, así como la prestación de un servicio satisfactorio.

Ejemplos de PET son:

- La disociación automática de los datos (anonimización):

Los datos se deben almacenar de forma tal que permitan identificar al sujeto afectado solo durante el tiempo mínimo e imprescindible que requiera la tarea para la que los datos fueron recopilados originalmente, procediendo a disociar los datos del mismo una vez la tarea haya concluido o el usuario esté inactivo.

- El empleo de métodos de cifrado:

Que impidan el acceso y/o el tratamiento no autorizados, y por tanto ilícitos, de los datos personales publicados por el usuario.

- Anuladores de *cookies*:

El uso de anuladores de *cookies*, para impedir que los sitios web puedan instalar ficheros que recaben información acerca de los hábitos de navegación del usuario (por ejemplo).

- La Plataforma de Preferencias de Privacidad o P3P:

Permite a los usuarios obtener un informe de las políticas de privacidad de las páginas web que visita y de si se ajustan o no a la normativa aplicable.

La plataforma establece un formato estándar para declarar la identidad y las prácticas sobre la información de los usuarios. Esta información puede ser interpretada por el usuario o, de forma automática, por software desarrollado a tal efecto.

Así, se pueden implementar herramientas (agentes de usuario) que permiten al usuario especificar sus preferencias y se encargan de comprobar automáticamente si lo especificado por el usuario se cumple para una página web determinada.

Dependiendo de las preferencias especificadas el agente puede por ejemplo mostrar un mensaje de alerta, generar una ventana para pedir instrucciones, permitir el acceso, rechazar el acceso... El proceso de comprobación de las preferencias se debe llevar a cabo en una zona segura en la cual el servidor web debe recoger sólo la mínima información posible del cliente.

- Los sistemas de gestión de identidad:

Que permiten al usuario controlar directamente los datos que revela sobre sí mismo en cada transacción, como los promovidos por el proyecto PRIME (Privacy and Identity Management for Europe).

Llegados a este punto haremos un breve repaso a la legislación española desde la Constitución Española hasta la LOPD que es la describe el tratamiento de datos de carácter personal dentro de España.

3.2.3 Legislación española

Constitución Española

29 de Diciembre de 1978

Artículo 17.

1. *Toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, sino con la observancia de lo establecido en este artículo y en los casos y en la forma previstos en la ley.*
2. *La detención preventiva no podrá durar más del tiempo estrictamente necesario para la realización de las averiguaciones tendentes al esclarecimiento de los hechos, y, en todo caso, en el plazo máximo de setenta y dos horas, el detenido deberá ser puesto en libertad o a disposición de la autoridad judicial.*
3. *Toda persona detenida debe ser informada de forma inmediata, y de modo que le sea comprensible, de sus derechos y de las razones de su detención, no pudiendo ser obligada a declarar. Se garantiza la asistencia de abogado al detenido en las diligencias policiales y judiciales, en los términos que la ley establezca.*
4. *La ley regulará un procedimiento de «habeas corpus» para producir la inmediata puesta a disposición judicial de toda persona detenida ilegalmente. Asimismo, por ley se determinará el plazo máximo de duración de la prisión provisional.*

Artículo 18.

1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*

2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
4. *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*

Artículo 20.

1. *Se reconocen y protegen los derechos:*

   a) *A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.*
   b) *A la producción y creación literaria, artística, científica y técnica.*
   c) *A la libertad de cátedra.*
   d) *A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.*

2. *El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.*
3. *La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España*
4. *Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.*

5. *Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.*

Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
5 de Mayo de 1982

Artículo 1.

1. *El derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo dieciocho de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas, de acuerdo con lo establecido en la presente Ley Orgánica.*
2. *El carácter delictivo de la intromisión no impedirá el recurso al procedimiento de tutela judicial previsto en el artículo 9º de esta Ley. En cualquier caso, serán aplicables los criterios de esta Ley para la determinación de la responsabilidad civil derivada de delito.*
3. *El derecho al honor, a la intimidad personal y familiar y a la propia imagen es irrenunciable, inalienable e imprescriptible. La renuncia a la protección prevista en esta ley será nula, sin perjuicio de los supuestos de autorización o consentimiento a que se refiere el artículo segundo de esta ley.*

Artículo 2.

1. *La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia.*
2. *No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso.*

3. *El consentimiento a que se refiere el párrafo anterior será revocable en cualquier momento, pero habrán de indemnizarse en su caso, los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas.*

Artículo 3.

1. *El consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil.*
2. *En los restantes casos, el consentimiento habrá de otorgarse mediante escrito por su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el Juez. [39]*

Respecto de esta ley Orgánica poco más podemos señalar, salvo que fue aprobada hace más de 30 años, y que el uso aquí contemplado, tal y como queda reflejado en el artículo 3, relativo a la cesión de derechos es hoy ineficaz de todo punto.

Si el consentimiento a menores e incapaces debe presentarse por escrito por parte del representante legal y este a su vez debe informar al Ministerio Fiscal, que tiene un plazo de ocho días para oponerse, es obvio que :

a) se ha quedado obsoleto por el uso de las TIC
b) no se cumple en la realidad objetiva.

Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

29 de Octubre de 1992

Esta ley Orgánica estuvo vigente hasta el 14 de enero de 2000. Con ella se trataba de dar cumplimiento al artículo 18.4 de la Constitución Española y supuso la primera norma en materia de protección de datos que se aprobó en España.

Para ello se estructura un sistema de garantías, que pretende recoger las orientaciones del Derecho comparado en materia de protección de datos personales.

El ámbito de aplicación de esta ley se circunscribe únicamente a los ficheros con datos personales que se tratan de forma automatizada.

La LORTAD concibe la protección de los bancos de datos personales funcionalmente, como una globalidad de procesos o aplicaciones que tratan los datos almacenados y que pueden ser susceptibles de configurar un papel personal más o menos completo si se interconectasen entre sí. No se limita, por tanto, a su tutela en tanto que nuevos depósitos de informaciones.

Para algunos expertos en Derecho, la LORTAD presentaba dos aspectos claramente positivos: la definición de los principios básicos, y el reconocimiento y tutela jurídica de la libertad informática, que se refiere a la facultad de acceso, modificación y control por parte de los ciudadanos de los datos que les son concernientes.

Así mismo sus significativas excepciones suponen un aspecto marcadamente negativo para esta ley, algo que se puede observar en la práctica totalidad de los artículos de la ley.

No entraremos más en detalle respecto de la derogada LORTAD, ya que tuvo corta vigencia, salvo para indicar, que en el Título VI (artículos del 34 al 41) de la mencionada ley se contempla la creación de un nuevo ente jurídico, la **Agencia**

Española de Protección de Datos (AEPD), que es la encargada de velar por el cumplimiento de esta Ley, aunque su estatuto no se publicaría hasta el año siguiente mediante el Real Decreto 428/1993, de 26 de marzo.

Fundamentada principalmente en la ***directiva 95/46/CE de la Comisión Europea*** de 1995 y actualizando la antigua LORTAD (como se verá, la LOPD mantiene vigentes múltiples aspectos de la derogada ley) a finales de 1999 se presenta la **Ley Orgánica de Protección de Datos de Carácter Personal**, que será de aplicación desde el 15 de Enero de 2000 en todo el territorio nacional. Es por tanto bajo el auspicio de esta ley que se ha experimentado el mencionado auge de las redes sociales online.

Además, de la LOPD, existen normas sectoriales en diversos ámbitos como sanidad o telecomunicaciones.

En lo referente a las RRSSO afectan principalmente las siguientes normas:

- **Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico** (LSSI-CE).
- **Ley 32/2003 General de Telecomunicaciones**.
- **Ley 25/2007 de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones**.
- **Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información**.

La LOPD nace con el fin de **proteger y garantizar las libertades y derechos fundamentales de las personas en lo relativo a su honor e intimidad, en lo concerniente al tratamiento de los datos personales**, y lo hace ampliando marcadamente el ámbito de aplicación de la ley con respecto a la anterior LORTAD, tal y como se describe en su Artículo 2.

Mientras la LORTAD tenía un ámbito bastante delimitado, a saber, únicamente se aplicaba a los ficheros que fuesen almacenados en algún tipo de soporte electrónico, que contuviesen datos de carácter personal, la LOPD amplía este ámbito a cualesquiera

sean los soportes en los que se almacenen los datos (incluyendo obviamente el tradicional formato "papel"), ya sean para procesamiento automatizado o no automatizado.

Sin duda, este artículo de la LOPD es una de las causas principales de la corta vida de la LORTAD, que apenas tuvo una vigencia de 7 años.

A modo de resumen de la LOPD, diremos que hay una serie de principios básicos aplicables a todo tratamiento de datos personales, sea este automático o no:

- Calidad de los datos:

  a) Los datos de carácter personal tratados deben ser adecuados, pertinentes y no excesivos, en relación con el ámbito y la finalidad para los que hayan sido recopilados.
  b) No pueden ser empleados para otras finalidades distintas.
  c) Deben ser veraces respecto de la situación **actual** de la persona afectada.
  d) Deben rectificarse en caso de constatarse errores en los mismos.
  e) Sólo pueden recabarse con fines determinados, explícitos y legítimos del responsable del tratamiento.
  f) No se permite la recogida de datos por medios fraudulentos, desleales o ilícitos.
  g) El responsable del tratamiento de los datos debe conservarlos únicamente mientras persista la finalidad con la se recogieron y cancelarlos al cese de la misma.

- Información en la recogida de datos:

En el artículo 5 de la ley, se indica que se debe informar al interesado del tratamiento que se va a realizar de sus datos personales en el momento en que se recaben sus datos, de forma expresa, detallada e inequívoca: de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad con la que se han recogido los datos, de los destinatarios de la información, de la identidad del responsable del tratamiento de los datos, de si es obligatorio o no otorgarlos y de su

posibilidad de ejercitar los derechos de acceso, oposición, cancelación y rectificación por parte del afectado.

- Datos especialmente protegidos:

Entre los que se incluyen la ideología, afiliación sindical, religión, creencias, origen racial, vida sexual, datos relativos a la salud así como los relacionados con la comisión de infracciones penales o administrativas.

- Seguridad de los datos:

Se recoge que las entidades (públicas o privadas que almacenen, traten o accedan a ficheros de datos personales deben aplicar medidas de seguridad para garantizar la disponibilidad, confidencialidad, e integridad de los datos.

- Deber de secreto:

Se obliga al secreto, custodia y confidencialidad de los datos a las entidades y personas que tratan y acceden a ficheros de datos de carácter personal.

- Comunicación de datos:

Los datos de carácter personal objeto del tratamiento sólo podrán comunicarse a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario y siempre previo el consentimiento del interesado.

- Acceso a los datos por cuenta de terceros:

Se contempla la prestación de un servicio al responsable del fichero por parte de un tercero, que accede a los datos del fichero para el cumplimiento de la prestación contratada; actuando en nombre, por cuenta y de acuerdo a las instrucciones establecidas y dadas por el Responsable del Fichero, ajustándose a criterios de protección similares a los que debiera emplear el responsable del fichero.

Respecto de la seguridad de los datos, el Título VIII del Reglamento de desarrollo de la LOPD establece las medidas que debe adoptar el responsable del tratamiento del fichero.

Entre estas medidas, se encuentra la elaboración de un documento que recogerá las medidas de índole técnica y organizativa acorde a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

Para ello, la AEPD facilita una guía de seguridad accesible en su web. [A]

Para no extendernos más, simplemente me gustaría indicar que la AEPD, cuyas atribuciones se describen en el artículo 35 y siguientes da cumplimiento al **artículo 8 de la *Carta de los Derechos Fundamentales de la Unión Europea*** del año 2000 en tanto que es la mencionada "*autoridad independiente*" que vela por el cumplimiento de estas normas en España.

Real Decreto Legislativo 1/2007

Como hemos comentado con anterioridad con la aparición de Internet, pero especialmente con el auge de las redes sociales, la forma de concebir el mercado ha cambiado: Si antes éramos nosotros como consumidores los que acudíamos a los comercios en busca de bienes y servicios, ahora son ellos los que nos buscan a nosotros a través de las plataformas de las redes sociales (además, brindándonos servicios a la carta, específicos para nuestro perfil como consumidores de acuerdo a lo ya expuesto en puntos anteriores de este documento).

Para asegurar los derechos de consumidores y usuarios en la adquisición de bienes y servicios a través de estos nuevos canales, surge el ***Real Decreto Legislativo 1/2007*** de 16 de Noviembre, que no es sino una puesta al día (en realidad una refundición) de la Ley General para la Defensa de los Consumidores y Usuarios

(26/1984) y otras leyes complementarias para regularizar, aclarar y armonizar los textos legales en lo referente a la contratación a distancia de productos y servicios.

Este RD tiene rango de ley, por lo cual es de aplicación directa y establece el "marco legal" de protección de los derechos de los consumidores y usuarios con carácter general desde el momento de su aprobación.

Entendemos por "**contrato a distancia**" a un mecanismo particular de negociación, distribución o contratación, en el cual el mensaje impreso (en una web, por ejemplo) o transmitido a distancia (vía telefónica…) constituye el mecanismo principal para ofrecer los productos o servicios a una clientela indeterminada y potencial de futuros consumidores.

Se trata de una operación que se desarrolla en tres fases o etapas fundamentales:

1. El consumidor recibe la oferta del producto o servicio mediante una técnica de comunicación a distancia, a través de una descripción escrita, visual u oral, con indicación del precio y demás condiciones de la oferta contractual.
2. Sobre esta base el consumidor efectúa su pedido, empleando también una fórmula cualquiera de comunicación a distancia para entrar en contacto con el vendedor.
3. Posteriormente recibe el producto o servicio en la dirección suministrada.

Debido a esta doble utilización de técnicas de comunicación, no se produce la presencia física simultánea del consumidor (contratante) y del proveedor (profesional), característica diferenciadora fundamental entre los contratos celebrados a distancia con respecto a los contratos habituales.

Quizá una de las diferencias más significativas es que al consumidor se le concede un período para privar de eficacia al contrato, mediante el desistimiento unilateral con el objeto de poder examinar con tranquilidad el producto comprado o determinada característica del servicio contratado.

Esta potestad se concede ya que el mencionado producto o servicio no se encuentra presente para su evaluación en el momento de la contratación. [40]

Llegados a este punto, vamos a revisar el derecho a la Propiedad Intelectual y en qué leyes se sustenta.

En España se creó la Ley de Propiedad Intelectual (LPI) en 1996 para incluir en el Derecho Civil los derechos de propiedad sobre las obras y creaciones artísticas, científicas y literarias.

Real Decreto Legislativo 1/1996
Ley de Propiedad Intelectual

Este Real Decreto, modificado en Enero de 2015 (Ley 21/2014), es el que se ha tenido en cuenta para determinar la extensión de los derechos de propiedad intelectual en España al refundir el texto de la Ley de Propiedad Intelectual (LPI).

En ella se recoge en su artículo primero que el derecho de la obra es única y exclusivamente del autor y lo es por el mero hecho de ser el creador de la obra [41]:

Artículo 1.

La propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación.

Para determinar quién es el autor de la obra, podemos acudir al artículo 5:

Artículo 5.

1. *Se considera autor a la persona natural que crea alguna obra literaria, artística o científica.*
2. *No obstante, de la protección que esta Ley concede al autor se podrán beneficiar personas jurídicas en los casos expresamente previstos en ella.*

Si queremos conocer qué derechos se le reconocen al autor éstos se encuentran detallados en los artículos 2 y 3:

Artículo 2.

La propiedad intelectual está integrada por derechos de carácter personal y patrimonial, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas en la Ley.

Artículo 3.

Los derechos de autor son independientes, compatibles y acumulables con:

1. *La propiedad y otros derechos que tengan por objeto la cosa material a la que está incorporada la creación intelectual.*
2. *Los derechos de propiedad industrial que puedan existir sobre la obra.*
3. *Los otros derechos de propiedad intelectual reconocidos en el Libro II de la presente Ley.*

Además en la ley se recogen los derechos de los autores, ya sean estos morales o de explotación, tal y como se recoge en los siguientes artículos:

Artículo 14.

Contenido y características del derecho moral.

Corresponden al autor los siguientes derechos irrenunciables e inalienables:

1. *Decidir si su obra ha de ser divulgada y en qué forma.*
2. *Determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente.*
3. *Exigir el reconocimiento de su condición de autor de la obra.*
4. *Exigir el respeto a la integridad de la obra e impedir cualquier deformación, modificación, alteración o atentado contra ella que suponga perjuicio a sus legítimos intereses o menoscabo a su reputación.*
5. *Modificar la obra respetando los derechos adquiridos por terceros y las exigencias de protección de bienes de interés cultural.*
6. *Retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de derechos de explotación.*

   Si, posteriormente, el autor decide reemprender la explotación de su obra deberá ofrecer preferentemente los correspondientes derechos al anterior titular de los mismos y en condiciones razonablemente similares a las originarias.

7. *Acceder al ejemplar único o raro de la obra, cuando se halle en poder de otro, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda.*

   Este derecho no permitirá exigir el desplazamiento de la obra y el acceso a la misma se llevará a efecto en el lugar y forma que ocasionen menos incomodidades al poseedor, al que se indemnizará, en su caso, por los daños y perjuicios que se le irroguen.

Artículo 17.

Derecho exclusivo de explotación y sus modalidades.

Corresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizadas sin su autorización, salvo en los casos previstos en la presente Ley.

Artículo 18.

Reproducción.

Se entiende por reproducción la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o de parte de ella, que permita su comunicación o la obtención de copias.

Artículo 19.

Distribución.

1. *Se entiende por distribución la puesta a disposición del público del original o de las copias de la obra, en un soporte tangible, mediante su venta, alquiler, préstamo o de cualquier otra forma.*
2. *Cuando la distribución se efectúe mediante venta u otro título de transmisión de la propiedad, en el ámbito de la Unión Europea, por el propio titular del derecho o con su consentimiento, este derecho se agotará con la primera, si bien sólo para las ventas y transmisiones de propiedad sucesivas que se realicen en dicho ámbito territorial.*
3. *Se entiende por alquiler la puesta a disposición de los originales y copias de una obra para su uso por tiempo limitado y con un beneficio económico o comercial directo o indirecto.*

   Quedan excluidas del concepto de alquiler la puesta a disposición con fines de exposición, de comunicación pública a partir de fonogramas o de grabaciones

audiovisuales, incluso de fragmentos de unos y otras, y la que se realice para consulta in situ.

4. *Se entiende por préstamo la puesta a disposición de originales y copias de una obra para su uso por tiempo limitado sin beneficio económico o comercial directo ni indirecto, siempre que dicho préstamo se lleve a cabo a través de establecimientos accesibles al público.*

   Se entenderá que no existe beneficio económico o comercial directo ni indirecto cuando el préstamo efectuado por un establecimiento accesible al público dé lugar al pago de una cantidad que no exceda de lo necesario para cubrir los gastos de funcionamiento. Esta cantidad no podrá incluir total o parcialmente el importe del derecho de remuneración que deba satisfacerse a los titulares de derechos de propiedad intelectual conforme a lo dispuesto en el artículo 37.2.

   Quedan excluidas del concepto de préstamo las operaciones mencionadas en el párrafo segundo del apartado 3 y las que se efectúen entre establecimientos accesibles al público.

5. *Lo dispuesto en este artículo en cuanto al alquiler y al préstamo no se aplicará a los edificios ni a las obras de artes aplicadas.*

Artículo 20.

Comunicación pública.

1. *Se entenderá por comunicación pública todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas.*

No se considerará pública la comunicación cuando se celebre dentro de un ámbito estrictamente doméstico que no esté integrado o conectado a una red de difusión de cualquier tipo.

2. Especialmente, son actos de comunicación pública:

a) Las representaciones escénicas, recitaciones, disertaciones y ejecuciones públicas de las obras dramáticas, dramático-musicales, literarias y musicales mediante cualquier medio o procedimiento.

b) La proyección o exhibición pública de las obras cinematográficas y de las demás audiovisuales.

c) La emisión de cualesquiera obras por radiodifusión o por cualquier otro medio que sirva para la difusión inalámbrica de signos, sonidos o imágenes. El concepto de emisión comprende la producción de señales portadoras de programas hacia un satélite, cuando la recepción de las mismas por el público no es posible sino a través de entidad distinta de la de origen.

d) La radiodifusión o comunicación al público vía satélite de cualesquiera obras, es decir, el acto de introducir, bajo el control y la responsabilidad de la entidad radiodifusora, las señales portadoras de programas, destinadas a la recepción por el público en una cadena ininterrumpida de comunicación que vaya al satélite y desde éste a la tierra. Los procesos técnicos normales relativos a las señales portadoras de programas no se consideran interrupciones de la cadena de comunicación.

Cuando las señales portadoras de programas se emitan de manera codificada existirá comunicación al público vía satélite siempre que se pongan a disposición del público por la entidad radiodifusora, o con su consentimiento, medios de descodificación.

A efectos de lo dispuesto en los dos párrafos anteriores, se entenderá por satélite cualquiera que opere en bandas de frecuencia reservadas por la legislación de telecomunicaciones a la difusión de señales para la recepción por el público o para la comunicación individual no pública, siempre que, en este último caso, las circunstancias en las que se lleve a efecto la recepción individual de las señales sean comparables a las que se aplican en el primer caso.

e) La transmisión de cualesquiera obras al público por hilo, cable, fibra óptica u otro procedimiento análogo, sea o no mediante abono.

f) La retransmisión, por cualquiera de los medios citados en los apartados anteriores y por entidad distinta de la de origen, de la obra radiodifundida.

Se entiende por retransmisión por cable la retransmisión simultánea, inalterada e íntegra, por medio de cable o microondas de emisiones o transmisiones iniciales, incluidas las realizadas por satélite, de programas radiodifundidos o televisados destinados a ser recibidos por el público.

g) La emisión o transmisión, en lugar accesible al público, mediante cualquier instrumento idóneo, de la obra radiodifundida.

h) La exposición pública de obras de arte o sus reproducciones.

i) La puesta a disposición del público de obras, por procedimientos alámbricos o inalámbricos, de tal forma que cualquier persona pueda acceder a ellas desde el lugar y en el momento que elija.

j) El acceso público en cualquier forma a las obras incorporadas a una base de datos, aunque dicha base de datos no esté protegida por las disposiciones del Libro I de la presente Ley.

k) La realización de cualquiera de los actos anteriores, respecto a una base de datos protegida por el Libro I de la presente Ley.

3. La comunicación al público vía satélite en el territorio de la Unión Europea se regirá por las siguientes disposiciones:

a) La comunicación al público vía satélite se producirá únicamente en el Estado miembro de la Unión Europea en que, bajo el control y responsabilidad de la entidad radiodifusora, las señales portadoras de programas se introduzcan en la cadena ininterrumpida de comunicación a la que se refiere el párrafo d) del apartado 2 de este artículo.

b) Cuando la comunicación al público vía satélite se produzca en el territorio de un Estado no perteneciente a la Unión Europea donde no exista el nivel de protección que para dicho sistema de comunicación al público establece este apartado 3, se tendrá en cuenta lo siguiente:

1.º Si la señal portadora del programa se envía al satélite desde una estación de señal ascendente situada en un Estado miembro se considerará que la comunicación al público vía satélite se ha producido en dicho Estado miembro. En tal caso, los derechos que se establecen relativos a la radiodifusión vía satélite podrán ejercitarse frente a la persona que opere la estación que emite la señal ascendente.

2.º Si no se utiliza una estación de señal ascendente situada en un Estado miembro pero una entidad de radiodifusión establecida en un Estado miembro ha encargado la emisión vía satélite, se considerará que dicho acto se ha producido en el Estado miembro en el que la entidad de radiodifusión tenga su establecimiento principal. En tal caso, los derechos que se establecen relativos a la radiodifusión vía satélite podrán ejercitarse frente a la entidad de radiodifusión.

4. La retransmisión por cable definida en el párrafo segundo del apartado 2.f) de este artículo, dentro del territorio de la Unión Europea, se regirá por las siguientes disposiciones:

a) La retransmisión en territorio español de emisiones, radiodifusiones vía satélite o transmisiones iniciales de programas procedentes de otros Estados miembros de la Unión Europea se realizará, en lo relativo a los derechos de autor, de acuerdo con lo dispuesto en la presente Ley y con arreglo a lo establecido en los acuerdos contractuales, individuales o colectivos, firmados entre los titulares de derechos y las empresas de retransmisión por cable.

b) El derecho que asiste a los titulares de derechos de autor de autorizar la retransmisión por cable se ejercerá, exclusivamente, a través de una entidad de gestión de derechos de propiedad intelectual.

c) En el caso de titulares que no hubieran encomendado la gestión de sus derechos a una entidad de gestión de derechos de propiedad intelectual, los mismos se harán efectivos a través de la entidad que gestione derechos de la misma categoría.

Cuando existiere más de una entidad de gestión de los derechos de la referida categoría, sus titulares podrán encomendar la gestión de los mismos a cualquiera de las entidades.

Los titulares a que se refiere este párrafo c) gozarán de los derechos y quedarán sujetos a las obligaciones derivadas del acuerdo celebrado entre la empresa de retransmisión por cable y la entidad en la que se considere hayan delegado la gestión de sus derechos, en igualdad de condiciones con los titulares de derechos que hayan encomendado la gestión de los mismos a tal entidad. Asimismo, podrán reclamar a la entidad de gestión a la que se refieren los párrafos anteriores de este párrafo c), sus derechos dentro de los tres años contados a partir de la fecha en que se retransmitió por cable la obra protegida.

d) Cuando el titular de derechos autorice la emisión, radiodifusión vía satélite o transmisión inicial en territorio español de una obra protegida, se presumirá que consiente en no ejercitar, a título individual, sus derechos para, en su caso, la retransmisión por cable de la misma, sino a ejercitarlos con arreglo a lo dispuesto en este apartado 4.

e) Lo dispuesto en los párrafos b), c) y d) de este apartado 4 no se aplicará a los derechos ejercidos por las entidades de radiodifusión respecto de sus propias emisiones, radiodifusiones vía satélite o transmisiones, con independencia de que los referidos derechos sean suyos o les hayan sido transferidos por otros titulares de derechos de autor.

f) Cuando, por falta de acuerdo entre las partes, no se llegue a celebrar un contrato para la autorización de la retransmisión por cable, las partes podrán acceder, por vía de mediación, a la Comisión Mediadora y Arbitral de la Propiedad Intelectual.

Será aplicable a la mediación contemplada en el párrafo anterior lo previsto en el artículo 158 de la presente Ley y en el Real Decreto de desarrollo de dicha disposición.

g) *Cuando alguna de las partes, en abuso de su posición negociadora, impida la iniciación o prosecución de buena fe de las negociaciones para la autorización de la retransmisión por cable, u obstaculice, sin justificación válida, las negociaciones o la mediación a que se refiere el párrafo anterior, se aplicará lo dispuesto en el Título I, capítulo I, de la Ley 16/1989, de 17 de julio, de Defensa de la Competencia.*

Artículo 21.

Transformación.

1. *La transformación de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente.*

   Cuando se trate de una base de datos a la que hace referencia el artículo 12 de la presente Ley se considerará también transformación, la reordenación de la misma.

2. *Los derechos de propiedad intelectual de la obra resultado de la transformación corresponderán al autor de esta última, sin perjuicio del derecho del autor de la obra preexistente de autorizar, durante todo el plazo de protección de sus derechos sobre ésta, la explotación de esos resultados en cualquier forma y en especial mediante su reproducción, distribución, comunicación pública o nueva transformación.*

Terminaremos con el repaso a esta ley haciendo referencia al ***Artículo 25***, en que se contempla la **compensación equitativa por copia privada**, que no es otra cosa, sino el conocido como "***canon digital*"** implantado hace algunos años para compensar a los autores por las pérdidas en las que incurrían al ver sus derechos intelectuales vulnerados.

En cuanto a legislación internacional se refiere, la Organización Mundial de la Propiedad Intelectual (OMPI) tiene un tratado relativo a los derechos de autor, que entró en vigor en 2002: El **Tratado de la OMPI sobre Derecho de Autor** que fue concluido en 1996.

En él se indica que cualquier parte contratante (aunque no esté obligada por la Convención de Berna para la Protección de las Obras Literarias y Artísticas) debe acatar las disposiciones sustantivas de la Ley de la Convención de Berna de 1971 (París).

En lo referente a los temas que son protegidos por medio de derechos de autor, el tratado menciona dos:

- Programas de computadora, cualquiera que sea la modalidad o la forma de su expresión,

- Compilaciones de datos u otros materiales ("bases de datos"), en cualquier forma, que en virtud de la selección o arreglo de su contenido constituyan creaciones intelectuales.

En lo referente a los derechos de autor, el tratado se ocupa de tres de ellos:

- El derecho de distribución,
- El derecho de alquiler
- El derecho de comunicación al público.

Cada uno de ellos es un derecho exclusivo, sujeto a ciertas limitaciones y excepciones.

El tratado obliga a las partes contratantes a proveer remedios legales contra la anulación de las medidas tecnológicas (p. ej., la codificación) que emplean los autores en el ejercicio de sus derechos y contra la remoción o alteración de información, como ciertos datos que identifican la obra de sus autores, que es necesaria para la administración (p. ej., otorgamiento de licencias, recolección y distribución de regalías) de sus derechos ("información sobre la administración de derechos").

El tratado obliga a cada una de las partes contratantes a adoptar las medidas necesarias, de acuerdo con su sistema legal, para garantizar la aplicación de dicho tratado. En particular, la parte contratante deberá asegurarse de que su ley incluya procedimientos que garanticen el cumplimiento, de modo que pueda instruirse una acción legal eficaz contra cualquier infracción de los derechos cubiertos por el tratado. Esa acción debe incluir remedios expeditos para prevenir la infracción y remedios que sean un factor disuasorio contra futuras transgresiones. [42]

Mientras la Propiedad Intelectual se reserva para la protección de las creaciones del espíritu en las que queda plasmada la personalidad del autor, tratándose de creaciones únicas y no producidas industrialmente o en serie (pueden ser obras literarias y artísticas como las novelas, poemas y obras de teatro, películas, obras musicales, obras de arte, dibujos, pinturas, fotografías…) la Propiedad Industrial protege todas las creaciones que están relacionadas con la industria: patentes y modelos de utilidad, signos distintivos y diseños.

Gracias a la Propiedad Industrial se obtienen unos derechos de exclusiva sobre determinadas creaciones inmateriales que se protegen como verdaderos derechos de propiedad.

En España hay varios tipos de derechos de Propiedad Industrial:

- **Diseños industriales**:

  Protegen la apariencia externa de los productos.

- **Marcas y Nombres Comerciales (Signos Distintivos)**:

  Protegen combinaciones gráficas y/o denominativas que ayudan a distinguir en el mercado unos productos o servicios de otros similares ofertados por otros agentes económicos.

- **Patentes y modelos de utilidad**:

  Protegen invenciones consistentes en productos y procedimientos susceptibles de reproducción y reiteración con fines industriales

- **Topografías de semiconductores**:

  Protegen el (esquema de) trazado de las distintas capas y elementos que componen un circuito integrado, su disposición tridimensional y sus interconexiones, es decir, lo que en definitiva constituye su "topografía".

Para cada uno de estos derechos hay una legislación aplicable, siendo los textos básicos los siguientes:

- Patentes y Modelos, **Ley 11/86 de patentes de invención y modelos de utilidad.**
- Signos Distintivos, **Ley 17/2001 de marcas.**
- Diseños Industriales **Ley 20/2003 de protección jurídica del diseño industrial.**
- Topografías de semiconductores **Ley 11/1988 de protección jurídica de las topografías de los productos semiconductores.**

Los derechos de Propiedad Industrial permiten a quien los ostenta decidir quién y cómo puede usarlos y se otorgan mediante un procedimiento por la Oficina Española de Patentes y Marcas y la protección que dispensan se extiende a todo el territorio nacional.

CAPÍTULO 4

DERECHOS, DELITOS, PELIGROS Y AMENAZAS EN LAS REDES SOCIALES

4.1 Derechos de los usuarios de las redes sociales online

De estas normas emanan una serie de derechos que tenemos como personas, consumidores y usuarios, que paso a enumerar brevemente:

4.1.1 Derecho a la libertad:

Recogido en el artículo 17 de la Constitución. La libertad de ser, de obrar, de pensar y de querer, es un derecho inherente a los seres humanos.

Desde las redes sociales pueden darse varias violaciones a este derecho, ya sea mediante amenazas y coacciones, que explicaremos en el próximo apartado (delitos en las redes sociales), e incluso la retención ilegal y el secuestro que, aunque no pueden darse directamente en las redes sociales, si pueden valerse de estas como herramienta, como en el caso del siguiente titular de prensa. [43]


Portada / Actualidad /

Facebook se usa para el secuestro y tráfico de menores en Indonesia

Publicado: 30 oct 2012 08:01 GMT | Última actualización: 30 oct 2012 08:44 GMT

4.1.2 Derecho a la intimidad:

Nos referimos al derecho a la intimidad ya sea esta personal o familiar, garantizado por el artículo 18 de la Constitución.

Este derecho puede ser vulnerado fácilmente en las redes sociales, incluso sin intencionalidad alguna, por parte de amigos o familiares, que etiqueten alguna foto en lugar íntimo (en el domicilio, por ejemplo), o que hagan alguna apreciación en su muro o emitan un tuit con información que no se desea dar a conocer por parte del afectado.

4.1.3 Derecho al honor:

El derecho al honor puede tener una significación relativa y ser valorado de manera diferente en razón de los grupos sociales.

El Tribunal Constitucional (TC) lo ha calificado como "concepto jurídico indeterminado". Esto es, que para poder llegar a su definición, debemos apoyarnos en otros conceptos.

El derecho al honor se relaciona con la reputación y fama de una persona, su prestigio profesional o su dignidad personal.

Este derecho puede vulnerarse vertiendo injurias y calumnias en las redes sociales, algo que explicaremos en el próximo apartado (Delitos en las redes sociales).

4.1.4 Derecho a la propia imagen:

El titular tiene derecho a impedir la difusión de su imagen pública. En lo relativo a las redes sociales este derecho se vulnera fácilmente. Basta con subir

cualquier archivo de video o imagen en la que una persona aparezca sin su consentimiento para poder vulnerarlo. Incluso puede verse más afectado con la posibilidad que brindan las redes sociales de etiquetar a las personas que aparecen en dicho video o foto.

4.1.5 Derecho a la información y libertad de expresión:

Tal y como se recoge en el artículo 20 de la Constitución todos tenemos derecho a emitir opiniones y a comunicar y recibir información veraz.

Este derecho tiene su limitación, como es lógico en los derechos del prójimo (su propio derecho de libertad de expresión, al honor, a la imagen propia, a la propiedad intelectual…).

Este derecho puede ser vulnerado cuando no se respetan las opiniones vertidas en las redes sociales.

Recientemente ha surgido cierta controversia ya que los algoritmos de control de alguna red social, no se permitía la publicación de ciertos contenidos ya que consideraba que no eran adecuados.

En este caso, un usuario pakistaní de la red social Facebook, criticaba el modo en que los occidentales empleaban su libertad de expresión para atacar a otras culturas.

Así mismo se han emitido quejas por la censura de fotografías relativas a la lactancia e incluso algunas de activistas relativas al cuerpo de la mujer o a la menstruación. [44]

4.1.6 Derecho a la propiedad intelectual e industrial:

Cada día millones de videos, fotografías y canciones se comparten en las redes sociales online a lo largo y ancho el planeta. En muy pocos casos se solicita la autorización del propietario de los derechos de la misma.

El problema es que se están lesionando los derechos de los creadores y la capacidad de reacción es escasa: Si un usuario difunde información protegida por los derechos de autor, la viralidad de la red hace que en poco tiempo un número casi exponencial de personas hayan podido acceder a él, difundirlo e incluso copiarlo o descargarlo.

Como se dice habitualmente las leyes van por detrás del crimen, y los medios técnicos actuales han demostrado no ser eficaces para la protección de estos derechos.

Además del material indicado protegido por derechos de autor de creadores y artistas, no podemos olvidar que nuestras fotos, videos, aportaciones o canciones, en definitiva, nuestras creaciones, también tienen derechos de propiedad intelectual y que nos pertenecen y pueden ser tan vulnerados como en los casos de autores profesionales.

Del mismo modo puede ocurrir con logotipos y marcas registradas, cuando se hace uso de las mismas sin consentimiento expreso. Como usuarios podríamos incluso ser denunciados en caso de que la compañía afectada considerase que hemos ocasionado algún perjuicio te su imagen corporativa (imagen de marca) ya que estaríamos lesionando su propiedad industrial.

Este derecho se ve amparado por la ley de Propiedad Intelectual.

4.1.7 Derecho al olvido:

El derecho al olvido es un derecho relacionado con el Habeas Data y la protección de datos de carácter personal.

Se puede definir como el derecho que tiene el titular de un dato personal a borrar, bloquear o suprimir información personal que se considera obsoleta por el transcurso del tiempo o que de alguna manera afecta el libre desarrollo de alguno de sus derechos fundamentales. Como cabe apreciar, este derecho puede en ocasiones colisionar con la libertad de expresión. [45]

En España, la LOPD regula el derecho al olvido en materia de ficheros de morosos en el art. 29.4 que dispone que "s**ólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos**".

¿Y en lo referente a los datos en Internet?

La magnitud de la red es tal que los datos se mantienen durante mucho tiempo, lo que añadido a la potencia de los indexadores de contenidos y motores de búsqueda de Internet que permiten localizar los datos fácil y rápidamente, así como la dispersión y replicación de datos hacen que la información pueda considerarse cuasi-perenne.

Imaginemos que en algún momento de nuestra vida fuimos multados, siendo este hecho publicado en el BOE o algún tipo de información que consideremos lesiva a nuestros intereses se publicó hace tiempo, **y ya no se ajusta a la situación actual**. Pues bien, hasta la aparición de este derecho, cualquiera podría realizar una búsqueda en Internet por nuestro nombre

(mediante un buscador como *Google*, *Yahoo!*, *Bing*…) y obtener esta información.

Téngase en cuenta que hablamos siempre bajo el supuesto de información veraz recogida en publicaciones legítimas, si no hablaríamos de la vulneración de otros derechos, no del derecho al olvido.

El derecho al olvido se sustenta en una sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de Mayo de 2014 que indica que los buscadores de Internet (no así los soportes originales) deben eliminar de sus resultados de búsqueda algunas entradas si son lesivas para el interesado, carecen de relevancia y no afectan a un personaje público a instancias del afectado.

Con la citada sentencia el TJUE dio respuesta a una cuestión prejudicial presentada por la Audiencia Nacional (AN) en 2012 acerca de la interpretación de las normas de protección de datos en Internet.

El alto tribunal precisa que el interesado debe presentar su solicitud "directamente" al buscador, que podrá examinar si es fundada. En caso de que el buscador no acceda a retirar la información, el afectado podrá acudir a la autoridad de control (la Agencia Española de Protección de Datos – AEPD - en el caso español) o a los tribunales para que estos lleven a cabo las comprobaciones necesarias y, en su caso, ordenen al buscador la retirada de la información.

Los buscadores de la red tienen desde entonces formularios de solicitud para las reclamaciones de los usuarios para solicitar el borrado de enlaces atendiendo a este derecho. [46]

El formulario para ejercer este derecho que habilita el buscador Google se encuentra recogido en el Anexo 1 de este documento.

En palabras del director de la AEPD, José Luis Rodríguez Álvarez (sic): "*Lo que hay que dejar claro es que esto <<el derecho al olvido>> no implica eliminar la información, implica que no sea accesible cuando se busca por el nombre de la persona afectada*".

4.2 Principales delitos en las redes sociales

Atendiendo a la legislación reseñada en el apartado previo, pasaremos a mencionar los delitos que más se cometen en las redes sociales e indicaremos los derechos contra los que atentan. De igual modo, trataremos de aportar un ejemplo del delito mencionado a través de titulares de prensa, preferiblemente española.

Llegados a este punto, lo primero sería buscar una definición adecuada al término *delito informático*. Una primera aproximación al término sería:

<<***Delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores medios electrónicos y redes de Internet***>>.

Parece que este término está un poco centrado en la informática en tanto que el objetivo del propio delito y no es la definición que buscamos.

Hay otra definición más amplia, de Rafael Fernández Calvo, que define el delito informático del siguiente modo:

<<***La realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos***>>.

Parece que esta definición si se ajusta más al tipo de delitos que se cometen diariamente en las redes sociales online.

Pasaremos ahora a desglosar los delitos uno a uno.

4.2.1 Delito de injurias:

Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves.

Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad.

4.2.2 Delito de calumnias:

Consiste en la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Hay que tener en cuenta que ambos atentan contra el honor de las personas. [47]

Se comete frecuentemente contra famosos y personas de la vida pública, pero también con personas de círculos cercanos (exparejas, compañeros, vecinos,…).

Hay que entender que en un contexto como el de las redes sociales, estos delitos se pueden cometer fácilmente, y que son difícilmente perseguibles. Aunque teóricamente el perfil de la persona en la red social debería permitir identificarla rápidamente no siempre es así: No todos los usuarios de las redes sociales usan perfiles completos y/o reales, por lo que la persecución de estos delitos telemáticos frecuentemente se alarga.

Cualquier comentario malintencionado puede servir para destrozar la reputación de una persona, y dado el carácter viral de las redes sociales y la habitualmente lenta y burocrática actuación de la justicia, puede hacer mucho daño, que será

difícilmente subsanado por desmentidos posteriores aplicando así aquello del refrán popular: “Difama que algo queda”.

La Brigada de Investigación Tecnológica (BIT) de la Policía Nacional reportó en 2012 más de 750 casos de delitos registrados de Injurias y calumnias en las redes sociales (un 200% más que en 2011). [48]

A continuación se recogen algunos titulares publicados en la prensa nacional como ejemplo:


Multado con 1.300 euros por injuriar a Cristina Cifuentes en las redes sociales

- La delegada del Gobierno en Madrid había solicitado cuatro años de prisión
- La Guardia Civil busca a 200 personas que enaltecen a ETA en redes sociales


Inicio » TEMA DEL DÍA » Internet y WhatsApp disparan un 24% las denuncias por injurias

Internet y WhatsApp disparan un 24% las denuncias por injurias

Las faltas por injurias son los hechos delictivos contra las personas que más crecen en el Camp de Tarragona por la actividad en Facebook y Twitter. Aún hay apariencia de impunidad


Civil

10 de Marzo de 2014

Condena a dos jóvenes toledanas por injuriar en Facebook y Tuenti

Incluye la sentencia

Dos jóvenes fueron condenadas a pagar una multa de 120 euros cada una al considerarlas un Juzgado de Instrucción de Toledo autoras criminalmente responsables de una falta de injurias por divulgar en las redes sociales Facebook y Tuenti insultos hacia otra tercera mujer que las denunció.

4.2.3 Delito de amenazas:

Comete un delito de **amenazas** la persona que anuncia o advierte a otra que le va a causar (a él/ella o su entorno, esto es, a su familia o alguien vinculado con él) un **daño** que pueda ser constitutivo de los delitos de homicidio, lesiones, torturas, daños al honor, a la intimidad, contra el patrimonio, o contra su integridad moral, entre otros, intimidando al amenazado y privándole de su propia tranquilidad y seguridad.

4.2.4 Delito de coacciones:

La **coacción**, por otra parte, se considera la violencia que se emplea para obligar a una persona a decir o hacer algo contra su voluntad, ya sea esta física, psíquica o moral.

Por tanto, será **coacción** todo ataque violento a la fase de ejecución de una voluntad y **amenaza**, todo ataque a la fase de formación de dicha voluntad.

Es decir, la diferenciación es temporal (una es previa a la otra) e incluso pueden darse juntas si el delito se prolonga lo necesario en el tiempo.

Para nuestra consideración los trataremos de modo indistinto y de forma conjunta.

En ocasiones, se tiende a pensar que las redes sociales son un mundo aparte, distinto del mundo real en el que nos movemos día a día, y que debido a ello, y al cierto grado de anonimato que éstas permiten, todo está permitido.

Así hay personas que amenazan a otras, ya sea por motivos ideológicos, políticos, de orientación sexual…, otras que reenvían (*retuitean*) *posts* de los que no se es el autor original, pero en los que se comete alguno de los mencionados delitos desconociendo, que independientemente de quien fuere el autor original, la responsabilidad sobre el mismo aplica al que lo publica.

Para hacernos una idea de lo normalizado que se encuentra este tipo de delitos, se observa que se cometen muy frecuentemente e incluso, no por personas anónimas, sino por todo tipo de entidades, como los partidos políticos, de los que salen los gobernantes que legislan sobre esta y otras materias.

A continuación se aportan algunos casos recientes recogidos en la prensa nacional [49]:

Ejemplo de amenazas por causa deportiva


EL MUNDO

Edición España Versión Clásica

SECCIONES | Deportes | Fútbol | Baloncesto | Ciclismo | Tenis | Fórmula 1 | Motociclismo

FÚTBOL Final de Copa

Imputan a un joven por amenazar con atentar en el Camp Nou

El joven, de 17 años, publicó comentarios en una red social diciendo que preparaba una bomba para "soltarla"en el estadio del Barcelona, durante la final de la Copa del Rey

Amenazas por causa ideológica o política, de diverso signo


MADRID / SUCESOS

«Qué ganas tengo de darte un tiro», nueva amenaza en Twitter a Cristina Cifuentes

Día 29/04/2014 - 11.45h


El PP denuncia amenazas desde el muro de 'Facebook' del PSOE de Güéjar Sierra

Publicado 13/02/2013 17:55:31 CET


Un concejal del PP, a Pablo Iglesias: "A ver si te dan un tiro en la nuca, cacho cabrón"

EL HUFFINGTON POST

Publicado: 07/11/2014 10:51 CET | Actualizado: 07/11/2014 16:59 CET

Amenazas por causa de orientación sexual

REDES SOCIALES

Un joven activista homosexual, amenazado de muerte en Twitter

Lambda, el colectivo LGTB valenciano, ha denunciado que uno de sus activistas de 18 años lleva varios días recibiendo amenazas de muerte

A continuación mostraremos un mensaje que se remitió por las redes sociales, originariamente twitter, pero también WhatsApp, Tuenti o Facebook, en el que, a modo de comentario gracioso se vierten amenazas contra la persona referenciada.

Sobre este tipo de mensajes cabe indicar que, además de poder ser constitutivos de un delito de incitación al odio, son responsabilidad del que los envía o postea, y no sólo del creador original del mismo:

Difusión en Twitter de amenazas contra Artur Mas, presidente de la Generalitat de Cataluña

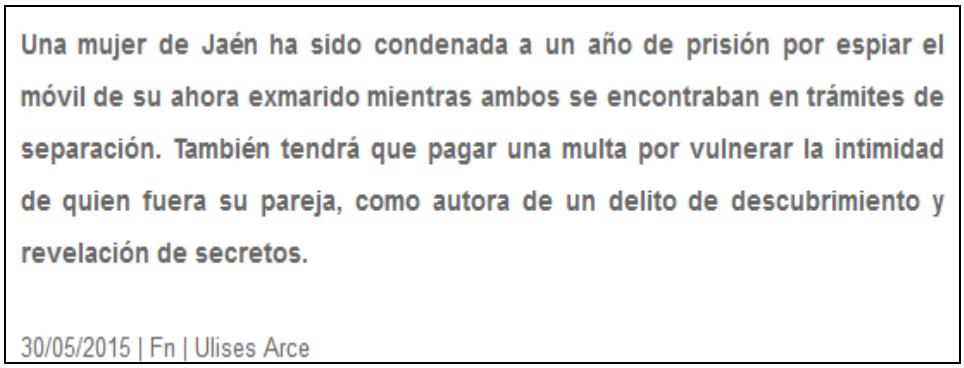
4.2.5 Lesión a la intimidad:

Se produce cuando información íntima e la persona se ve comprometida o robada por parte de un tercero. Esto incluye mensajes, correos, fotos, pero no se circunscribe únicamente a ellos.

Se aportan sendos ejemplos de vulneración de este derecho acontecidos recientemente en España [50]:

TS confirma la condena de 15 jóvenes que se pasaron un vídeo íntimo robado a una vecina

La afectada llevó su ordenador a una tienda de informática y un técnico descubrió en la 'papelera de reciclaje' un vídeo sexual. Las copias circularon por el pueblo, y hasta se organizaron proyecciones en la cocina de la taberna, la piscina municipal y entre los servicios de Protección Civil y los bomberos



Una mujer de Jaén ha sido condenada a un año de prisión por espiar el móvil de su ahora exmarido mientras ambos se encontraban en trámites de separación. También tendrá que pagar una multa por vulnerar la intimidad de quien fuera su pareja, como autora de un delito de descubrimiento y revelación de secretos.

30/05/2015 | Fn | Ulises Arce

4.3 Peligros y amenazas para los usuarios de las redes sociales

Además de los delitos indicados, o precisamente, en comisión de los mismos podemos encontrarnos varias amenazas.

4.3.1 Ciberacoso:

El ***acoso*** consiste en el hostigamiento y persecución de alguna persona por cualesquiera motivos con el fin de importunarla, molestarla, obtener favores sexuales…

Se contemplan multitud de tipos de acoso, entre otros los siguientes:

- ***Acoso sexual***, si se pretende conseguir algún tipo de favor de esa índole de la persona acosada.
- ***Acoso laboral*** (mobbing), cuando el acoso tiene lugar en el lugar de trabajo. Este puede provenir de un compañero o algún superior.
- ***Acoso escolar*** (bullying), se da entre jóvenes cuando se produce dentro del entorno escolar, en el que las víctimas son vistas como débiles por sus compañeros.

Existen otros tipos de acoso menos específicos, pero que pueden ser considerados como tal atendiendo a la intencionalidad del acosador y a los efectos en el acosado (acoso físico, moral,…).

Cuando el acoso se lleva a cabo a través de medios cibernéticos, tales como las redes sociales, correo electrónico, etc. hablamos de ciberacoso.

4.3.2 Ciberbullying:

Un caso bastante particular es el ***ciberbullying***, que no es sino el acoso escolar llevado a las redes.

Es de especial interés por diversos motivos:

1- La indefensión del acosado, pues generalmente se trata de menores.
2- El acosado y el acosador tienen contacto físico a lo largo del día en el centro escolar, por lo que la situación de acoso se puede prolongar fuera de las redes sociales incluso mediante amenazas físicas.
3- Las características de las redes sociales, hacen que el acoso pueda tener a cualquier hora y en cualquier lugar, debido a la versatilidad de acceso.

Este tipo de actitudes pueden desembocar en situaciones trágicas como un caso recientemente acontecido en Madrid [51]:

CASO ARANCHA ACOSO ESCOLAR »

Una adolescente discapacitada se suicida tras sufrir acoso escolar

- La familia de la menor, alumna de un instituto madrileño, había acudido a la policía
- El acoso escolar deja más secuelas que el maltrato por parte de adultos

PILAR ÁLVAREZ / ELISA SILIÓ / F. JAVIER BARROSO | Madrid | 23 MAY 2015 - 14:59 CEST

4.3.3 Grooming:

Otro caso de acoso peculiar es el ***grooming***, que definiremos como el conjunto de acciones que lleva a cabo una persona sobre un menor, con un objetivo marcadamente sexual. El objetivo puede tener como fin último desde la obtención de imágenes del menor en situaciones sexuales o pornográficas, hasta la posibilidad de

establecer contacto físico y presencial con dicho para consumar un abuso sobre éste. [52]

Hay que considerar como especialmente graves aquellas en las que la persona que ejerce el acoso forma parte del entorno del menor, incluyendo profesores, familiares, monitores… y una variante menos frecuente, pero que se está dando cada vez con mayor intensidad, que consiste en aquellos casos en los que el acosador también es un menor de edad.

A continuación se aporta un titular relativo a este tipo de situaciones [53]:


Un joven catequista de Cádiz, a la cárcel acusado de pederastia

• El agresor contactaba con los menores como "profesor" y los llevaba a merendar y al fútbol

4.3.4 Sexting:

El ***sexting*** consiste en la captación y envío de mensajes (originariamente de texto, SMSs), fotos o videos con alto contenido erótico o sexual entre un acosador adulto y un menor (habitualmente chicas).

Frecuentemente los videos o fotos son tomadas por parte del menor de forma consciente, sin tener idea del daño a su intimidad que las mismas suponen, y son entregadas efecto del acoso o engaños, o por otros motivos: coqueteo, como "regalo" a la pareja...

Habitualmente, el *sexting* viene acompañado de coacciones y amenazas relativas a la divulgación del contenido si no se accede a determinadas exigencias (económicas, sexuales).

Un aspecto a tener muy en cuenta es que ya se han dado algunos casos de *sexting* (al igual que se indicó para el *grooming*) en el que víctima y acosador eran menores, por lo que puede surgir asociado a ***ciberbullying.***

Si se analizan las causas del fenómeno del sexting, tenemos que hay cierta **falta de cultura de privacidad**, o si se quiere, cierto **afán de notoriedad** por el colectivo adolescente, lo que, sumado a **una menor conciencia de los riesgos**, o a un **exceso de confianza** (habitualmente por la "brecha digital", lo que convierte a los jóvenes en los entendidos en la materia tecnológica dentro del hogar), y al **despertar sexua**l de los adolescentes supone el caldo de cultivo idóneo para el surgimiento de estas prácticas.

De nuevo nos encontramos con un acoso cometido contra menores, y de nuevo es importante la indefensión del colectivo, a lo que hay que añadir el anonimato brindado por las redes sociales al acosador que puede usar un perfil falso. Estos casos acaban en ocasiones en unas situaciones dramáticas para las víctimas por lo que hay que estar muy pendiente de su detección precoz para una rápida solución del problema.

El acoso puede a su vez contemplarse desde la comisión de otros delitos, algunos ya mencionados: calumnias, injurias, amenazas, coacciones, pero también mediante otros, como son la suplantación de personalidad o el robo de datos.

Ejemplos de acciones de ciberacoso serían:

- Acceder a sus cuentas y modificar claves para impedir el acceso, robar fotografías o archivos, o leer mensajes de la cuenta.
- Acceder de forma ilegal para suplantar a la persona e interactuar en la red social como si de ella se tratase.
- Crear perfiles falsos del acosado con diversos fines: insultar a otros usuarios, crear mensajes ofensivos,… para que las reacciones adversas recaigan sobre la víctima.
- Colgar material audiovisual del acosado en actitudes comprometidas, ya sea este material real o no, y ponerlo en conocimiento de su entorno para avergonzarlo o atacar a su honor.

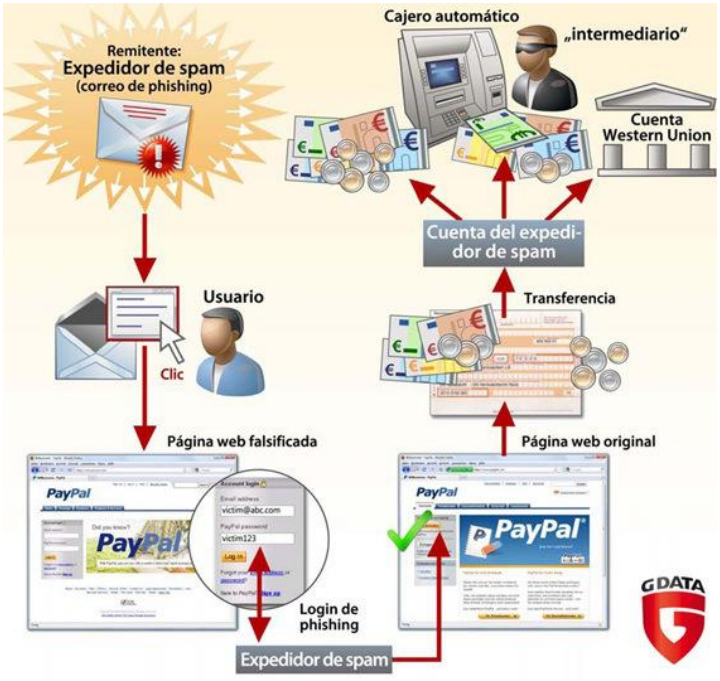
4.3.5 Suplantación de identidad (phishing):

Consiste en la suplantación de la persona de modo online. Habitualmente se hace llegar a la víctima un vínculo a un sitio web fraudulento que aparente ser otro en la

víctima confía: un banco, un proveedor de correo, una web de servicios de telefonía… con el objetivo de obtener sus datos personales (clave de cuenta de correo, PIN de tarjeta bancaria…) para acometer otras acciones delictivas: Solicitar un crédito en su nombre, robar dinero de su cuenta, obtener documentos oficiales en su nombre, abrir cuentas nuevas en su lugar.

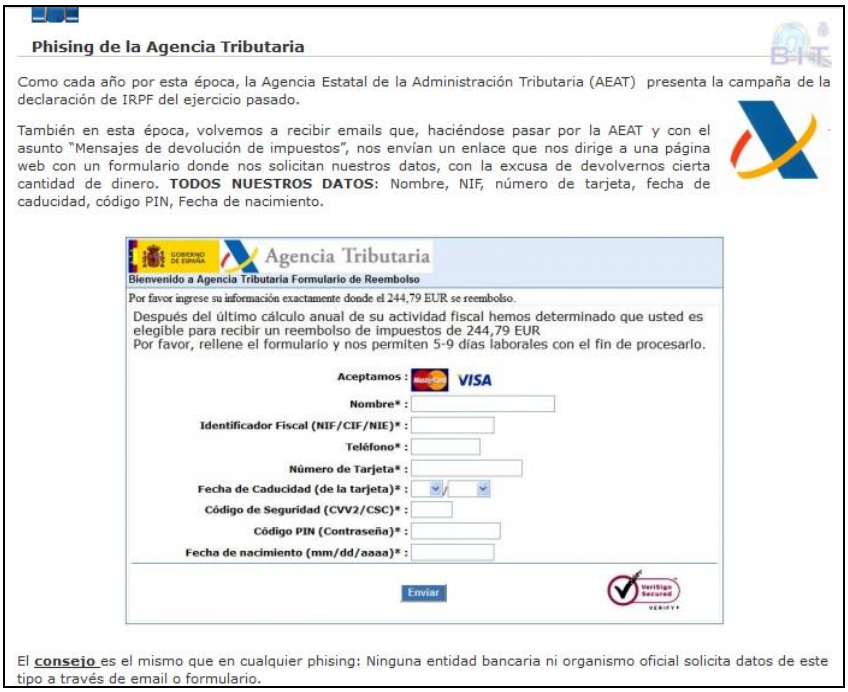
A continuación se aporta un diagrama en el que se recoge el funcionamiento habitual de un proceso de phishing.

Fig.5 - Representación gráfica de un proceso de phishing



Se aporta a modo de ejemplo uno de los últimos casos de phishing que ha sufrido la AEAT [54]:

Fig.6 – La AEAT víctima de phishing



4.3.6 Pharming:

El ***pharming*** es otra forma de suplantación muy similar al phishing, cuya única diferencia radica en que la suplantación se efectúa en el servidor de DNS (el lugar donde se relacionan las IPs y los dominios) reemplazando la correlación del dominio afectado por una IP en la que se encuentra una web falsa con la misma apariencia que la afectada para así conseguir los datos de la víctima cuando intenta acceder.

4.3.7 Tabnabbing:

El ***tabnabbing*** es una nueva técnica de phishing basada en la funcionalidad de pestañas (tabs) de los navegadores modernos descubierta por *Aza Rashkin*, un desarrolladro del navegador *Mozilla.*

El funcionamiento es el que sigue: cuando el usuario se mueve entre pestañas, se cambia el aspecto de la que no queda visible para que se parezca a alguna página de

acceso a servicios (*Google*, *Yahoo*!, *Facebook*, *Twitter*…) e indicamos que la sesión se ha cerrado a causa de la inactividad.

El usuario, que no se percata, introduce nuevamente sus datos de acceso a la plataforma que, de este modo, se encuentran ya en poder del cibercriminal. [55]

Cabe indicar que hay otras muchas formas de suplantar la identidad de alguien: crear un perfil y hacerlo pasar como el de otra persona, por ejemplo.

Los fines de esta suplantación pueden ir desde ejercer algún tipo de acoso hasta la obtención de datos por parte de su círculo de amigos o familiares.

4.3.8 Sabotaje o daño informático:

En ocasiones se remiten a los usuarios mensajes con técnicas de ingeniería social menajes para la descarga de ejecutables (*bots*, *troyanos*) en su dispositivo. El funcionamiento es relativamente sencillo pues es la víctima quien voluntariamente acepta la instalación del programa. Estos programas pueden servir para la recopilación de datos el usuario, e incluso causar daños permanentes en los equipos en los que son instalados.

4.3.9 Fraude informático:

Un fraude es una forma de obtener algún beneficio eludiendo las disposiciones legales en prejuicio de un tercero.

De forma habitual se dan pequeñas estafas en las que se reclama una cantidad de dinero a las víctimas para algún fin, aunque el dinero no se destine a ello.

4.3.10 Clickjacking:

Es un *malware* (software malicioso) basado en un fallo de diseño de HTML que pretende engañar al usuario con la finalidad bien de obtener información

confidencial, bien de tomar el control de su dispositivo al hacer click sobre algún enlace.

El fin del *clickjacking* es conseguir que un usuario pulse en un enlace (y realice una acción) sin que lo sepa, o creyendo que lo hace en otro enlace con otra finalidad.

Los resultados van desde hacerse seguidor de alguien en Twitter, marcar un "Me gusta" en Facebook o algunos más graves como dar el consentimiento para cualquier tipo de acción.

4.3.11 Cookies:

Aunque todos estamos habituados ya a los cuadros de diálogo acerca del uso de cookies por parte de los sitios web, en ocasiones estas se instalan sin conocimiento del usuario.

Tan sólo indicar, que aunque habitualmente como usuarios de redes sociales online y otros sitios web aceptemos el uso de cookies la mayoría de los usuarios desconocen a qué se está dando consentimiento realmente, pues las cookies sirven para proporcionar información acerca de nuestra navegación web, del dispositivo desde el que nos conectamos, de su ubicación, del tiempo que hemos estado navegando… Es decir, aportan mucha información y muy diversa acerca de nuestros hábitos y nuestro comportamiento, pero también otra de índole técnica, como el navegador que empleamos o el sistema operativo desde el dispositivo empleado, datos que son bastante útiles si se desea llevar a cabo cualquier acción malintencionada contra nosotros.

4.3.12 Social spammer:

Las redes sociales brindan una posibilidad inmejorable para el envío masivo de mensajería con fines comerciales o spam. Aunque esta práctica está en desuso (para ver el motivo hay que recordar lo expuesto en cuanto al Marketing 3.0), es cierto que hay casos frecuentes, y no solo de spam, sino de scam (mensajes que persiguen un lucro indebido mediante fraude o estafa).

Aunque pueden reportarse los usuarios que hacen este scam para la cancelación de las cuentas por parte del proveedor de servicios, hay en twitter una situación particular, que es la remisión de este spam desde cuentas, llamémoslas virtuales, creadas para este único fin y que por tanto no tienen una persona detrás con afán de otro tipo de interacción social, o desde cuentas robadas, es decir cuentas de las que un pirata ha conseguido la clave y que son usadas con este fin. [56]

4.3.13 Apología de la anorexia y la bulimia:

Existen en las redes sociales cuentas y perfiles que promueven la anorexia y/o la bulimia. Estos trastornos alimenticios de origen neurótico son particularmente peligrosos para los menores (en concreto las chicas son las que más las sufren) y son muy peligrosos para la salud, pudiendo causar incluso la muerte.

La principal forma de atajar estos problemas es mediante apoyo psicológico constante para evitar que las jóvenes recaigan y fortalecer su autoestima, motivo por el cual estas cuentas o perfiles son altamente peligrosos, ya que anulan los esfuerzos de familia y profesionales para corregir la situación, ya que las jóvenes se sienten apoyadas y sustentadas en la red, lo que las fortalece en su convicción de no comer o provocarse el vómito.

En este sentido, estos grupos "tóxicos" hacen una función inversa a la de los grupos de apoyos (alcohólicos anónimos, ludopatía…).

Hace unos años se localizaron perfiles en Facebook a este respecto que fueron eliminados por la plataforma [57]:


CONSEJOS DE BITDEFENDER 27/08/2011

Anorexia y bulimia: perfiles de Twitter y Facebook las promueven

4.3.14 Apología de terrorismo:

En las redes sociales también pueden encontrarse personas o grupos que hacen apología del terrorismo (yihadismo) o del uso de la violencia.

Desgraciadamente, también tenemos ejemplos recientes para este caso. [58]

APOLOGÍA DEL TERRORISMO »

Detenido un joven por difundir una decapitación en redes sociales

- El varón de 18 años escribió que lo mismo debía hacerse con políticos y policías
- La grabación recoge un asesinato yihadista, según la Guardia Civil

4.3.15 Pedofilia y pornografía infantil:

Las redes sociales no son sino reflejo de la sociedad en qué vivimos, por lo que también encontramos en ella estas dos lacras.

Se trata de grupos de adultos que comparten material fotográfico o videos de menores desnudos, con poca ropa o en actitudes o posturas que inciten su libido (pornógrafos).

En algunas ocasiones estas personas incluso intentan contactar con los menores mediante solicitudes de amistad e incluso entablar encuentros con los mismos, e incluso acosan y amenazan a los menores para conseguir sus fines. [59]

PGJEM investiga video de presunto pedófilo en redes sociales

El ministerio público del fuero común está tomando comunicación con los familiares de algunas víctimas para que haya una imputación directa hacia este individuo identificado como Marcial Navarrete.

POR: AGENCIAS | 17 / FEBRERO / 2015 - 04:58 P.M. | COMPARTIR

4.3.16 Difusión de datos personales:

Como ya se ha indicado, uno de los mayores problemas de las Redes sociales es que nuestra información está expuesta a miradas ajenas: nuestro lugar de trabajo, de residencia, nuestras amistades y familiares, nuestros gustos o tendencias, incluso, si se presta atención, pueden conocerse horarios de trabajo y localizaciones de la persona, esto puede desembocar en acoso o suplantación de identidad (ya referidos) e incluso en robos, secuestros o asesinatos.

Se aportan titulares de varias noticias de prensa al respecto. [60]

Facebook reconoce haber rastreado por error a usuarios ajenos a la red social

- Todo se debió a un "fallo" que provocaba el emplazamiento de cookies en webs.
- No era nuestra intención. Se está trabajando en arreglarlo", indicó en un comunicado un directivo de la compañía.
- El directivo asegura que Facebook es "transparente" en el uso de cookies.

EFE. 10.04.2015 - 17:49h

Facebook reconoció este viernes haber rastreado por error a internautas ajenos a la red social, debido a un "fallo" que provocaba **el emplazamiento de cookies en páginas web.**

Detenida una banda que buscaba en Facebook información para sus robos

Tags: Seguridad

Si usted está en Facebook, tenga cuidado con las actualizaciones de estado. En Estados Unidos tres personas han sido detenidas por robar en casas en las que los dueños habían publicado en su página de Facebook que no iban a estar en sus hogares.

ASHLEY MADISON »

Publicados los datos de 39 millones de infieles registrados en Ashley Madison

- La información de una de las webs más importantes en la búsqueda de sexo extramatrimonial fue robada por piratas en julio
- Los peores ataques cibernéticos de EEUU

EL PAÍS | Madrid | 20 AGO 2015 - 16:51 CEST

ESPAÑA / CRIMEN DE CUENCA

La supuesta boda de Marina Okarynska pudo desencadenar el crimen de Morate

S. E. / MADRID | Día 21/08/2015 - 21.05h

En esta última noticia, y dado que no se indica en el titular, parece que el desencadenante del crimen es la difusión de las fotos de la boda de la víctima a través de las RRSSO.

4.3.17 Violencia de género:

Las redes sociales también sirven para ejercer violencia de género ya que a través de ellas puede llegar a saberse dónde está una persona en cada momento, con quién está hablando, que lleva puesto (mediante el posteo de fotografías…).

En ocasiones la parte maltratadora de la pareja (habitualmente el hombre) puede ejercer dominio e incluso violencia psicológica sobre la víctima, ya sea mediante las redes sociales o físicamente, en la vida cotidiana, por algún contenido publicado en ellas.

A continuación algunas preguntas indicativas de un posible problema de maltrato de género que habitualmente se ignoran con excusas cómo: “los chicos son así” o “es que se interesa por ti”:

- “¿Quién es éste al que le gusta tu foto?”.

- "No enseñes tanto, ponte otra ropa".
- "¿Qué hacías en este sitio?"
- "¿Estás sola?"

Incluso se pueden dar otras situaciones, como demandar a la pareja la clave de acceso ("¿si no tienes nada que ocultar por qué no me la das?"), pudiendo pasar así del control a otras situaciones: suplantación de identidad, chantajes mediante amenazas y coacciones ("si me quisieras no tendrías amigos chicos" o "si me abandonas publicaré las fotografías que tú sabes…"), ciberacoso mediante el envío constante de mensajes... Como ya hemos visto, es relativamente fácil (e incluso frecuente) ejecutar unos delitos en la presencia de otros.

4.3.18 Geolocalización y geoetiquetado:

Otro de los riesgos consiste en revelar nuestra localización, algo posible mediante herramientas de geolocalización y geoetiquetado para el contenido multimedia que compartimos, lo que permite localizarnos para la comisión de cualquier tipo de delito.

Actualmente, las RRSSO más populares como *Facebook*, *Instagram* o *Twitter* disponen de herramientas que eliminan de forma automática este tipo de datos de las fotografías que se comparten en sus plataformas.

Introduciremos aquí un peligro que aunque no proviene de acciones malintencionadas de terceros no por ello deja de ser bien cierto.

4.3.19 Adicción a las redes sociales:

Actualmente, y debido al uso de dispositivos móviles podemos estar conectados a Internet y las redes sociales 24 horas al día. En casa, en el metro, en la cola de un banco… podemos estar (y en ocasiones lo estamos) conectados a juegos, aplicaciones o simplemente conectados a grupos de WhatsApp u otras RRSSO como *Facebook* o *Twitter*.

De la **posibilidad** de usar las redes sociales en cualquier momento ha surgido la **necesidad**, de modo que hay personas que necesitan sentirse "online" continuamente.

Estas actitudes pueden ser muy negativas ya que pueden generar falta de ansiedad, estrés e incluso depresión.

Por último, indicar que este problema afecta generalmente a los más jóvenes (niños y adolescentes), que son más activos con el uso de las nuevas tecnologías y a la vez son un colectivo con menor madurez y mayor indefensión. [61]

4.3.20 Dolencias físicas:

Muy relacionado con el anterior. Introducimos aquí un riesgo derivado del uso de la tecnología y las redes sociales que son aquellas dolencias físicas puede acarrear su uso continuado, tales como dolores musculares, vista cansada y hasta problemas óseos.

Por ejemplo, se calcula que pasamos entre 700 y 1400 horas al año con la cabeza agachada haciendo uso de dispositivos móviles, cifra que aumenta en los adolescentes, lo que causa problemas cervicales al adoptar la que en términos médicos ya se conoce como postura del *WhatsApp*.

Según un reciente estudio del cirujano ***Kenneth K. Hansraj*** titulado ***Assessment of Stresses in the Cervical Spine Caused by Posture and Position of the head,*** adoptamos una postura que, atendiendo al centro de gravedad y al peso medio de la cabeza de un adulto (unos 6 kg.) nos hace soportar fuerzas en el cuello que van desde los 12 kg a unos 12º de inclinación hasta 27 kg a 60º.

4.4 Peligros y amenazas para los proveedores de servicios de las redes sociales

Pudiera parecer que los proveedores de servicios tienen cierta responsabilidad en algunas de estas situaciones, y en ciertos casos es así, pero ellos también se ven atacados en ocasiones.

Recogemos algunos de los ataques más frecuentes que sufren. [62]

4.4.1 Denegación de servicio (DoS):

Los proveedores de servicios que sufren este tipo de ataques ven como sus "*sites*" son colapsados por los "*crackers*" de modo que no puedan prestar sus servicios con normalidad (e incluso no puedan prestarlos en absoluto).

Este tipo de ataques se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no dé abasto a la cantidad de solicitudes. Para ello emplean los protocolos TCP/IP, de diversas formas para saturar los recursos de los servidores afectados. Algunos de ellos son: "*SYN Flood", "ICMP flood"* o *"Service Port flood"*.

La mejor forma de protegerse de estos ataques consiste en:

- Limitar la tasa de tráfico proveniente de un único *host*.
- Limitar el número de conexiones concurrentes al servidor.
- Restringir el uso del ancho de banda por aquellos *hosts* que cometan violaciones.
- Realizar un monitoreo de las conexiones TCP/UDP que se llevan a cabo en el servidor (permite identificar patrones de ataque).

Además existen algunas herramientas comerciales que permiten paliar este tipo de situaciones (*Site Defender*…).

4.4.2 Ataques a bases de datos:

Otro tipo de ataques son aquellos que se dan no con la intención de interrumpir la prestación del servicio, sino con la intención de extraer datos, modificarlos o eliminarlos.

La técnica más extendida es la Inyección SQL, consistente en la inserción de un código SQL (invasor), dentro del programado con el fin de alterar el funcionamiento normal del programa y lograr así que se ejecute en base de datos la porción de código "invasor".

En el Anexo 2 se describe el funcionamiento de este ataque, así como algunas de las defensas más habituales que pueden emplearse para evitarlo. [63]

4.4.3 Ataques internos:

En otras ocasiones, el ataque al proveedor de servicios puede incluso provenir de dentro, de algún empleado de la empresa o persona cercana a esta.

En este caso, los atacantes aprovechan su posición de confianza con la empresa para poder realizar el acto (sabotaje, robo…).

A continuación en ejemplo de un robo de información de estas características aparecido recientemente en la prensa que, aunque no es relativo a una red social, pudiera haberlo sido por su *modus operandi [64]*:

EL PAÍS

ECONOMÍA

ECONOMÍA EMPRESAS MERCADOS BOLSA MIS AHORROS VIVIENDA TECNOLOGÍA

Morgan Stanley despide a un empleado que robó datos de 350.000 clientes

• El banco de negocios dice que el uso de la información no ha causado ningún perjuicio económico

SANDRO POZZI | Nueva York | 5 ENE 2015 - 18:53 CET 3

Aunque esos casos no son demasiado frecuentes (o al menos no transcienden con frecuencia, es cierto que se producen y que están fuertemente penados por la ley [65]:

Tres años de prisión por robar y revelar información de su empresa

Twittear 1 Compartir 71 g+1 Compartir

Más noticias sobre: juridico, empresas

07.01.2011 Victoria Martínez-Vares 2

Un tribunal condena a un ingeniero por sustraer de la consultora en la que trabajaba información confidencial y ponerla a disposición de la compañía a la que se incorporó poco después.

Es importante tener en cuenta que las penas pueden diferir enormemente dependiendo de la edad que tenga la persona que las comete, así, y tal y como se recoge en la Ley Orgánica 10/1995 referente a la implantación del Código penal:

<<Esta norma es de aplicación a sujetos mayores de edad y, excepcionalmente, a sujetos menores en edad comprendidos entre los dieciséis y dieciocho años>>.

Del mismo modo, la Ley Orgánica de Responsabilidad Penal de los Menores del 12 de Enero del año 2000, es la que debe aplicarse a los menores comprendidos entre los 14 y los 18 años y que puede ser aplicada a menores de 21 a criterio judicial, dependiendo de su grado de madurez.

4.5 Peligros y amenazas para los proveedores de servicios de las redes sociales

Como ya se ha indicado, los proveedores de servicios también sufren ataques, pero además, también son los primeros en poner los medios para la defensa de sus usuarios (clientes) frente a los mismos.

Como es comprensible, los principales interesados en que nuestra experiencia como usuarios se gratificante y que no desemboque en situaciones indeseables son los proveedores del servicio, ya que si los usuarios identifican las plataformas con una fuente de peligro lo más probable es que la abandonen rápidamente.

Pasamos a detallar algunas de las medidas que los administradores de los *sites* de redes sociales toman para intentar paliar este tipo de situaciones.

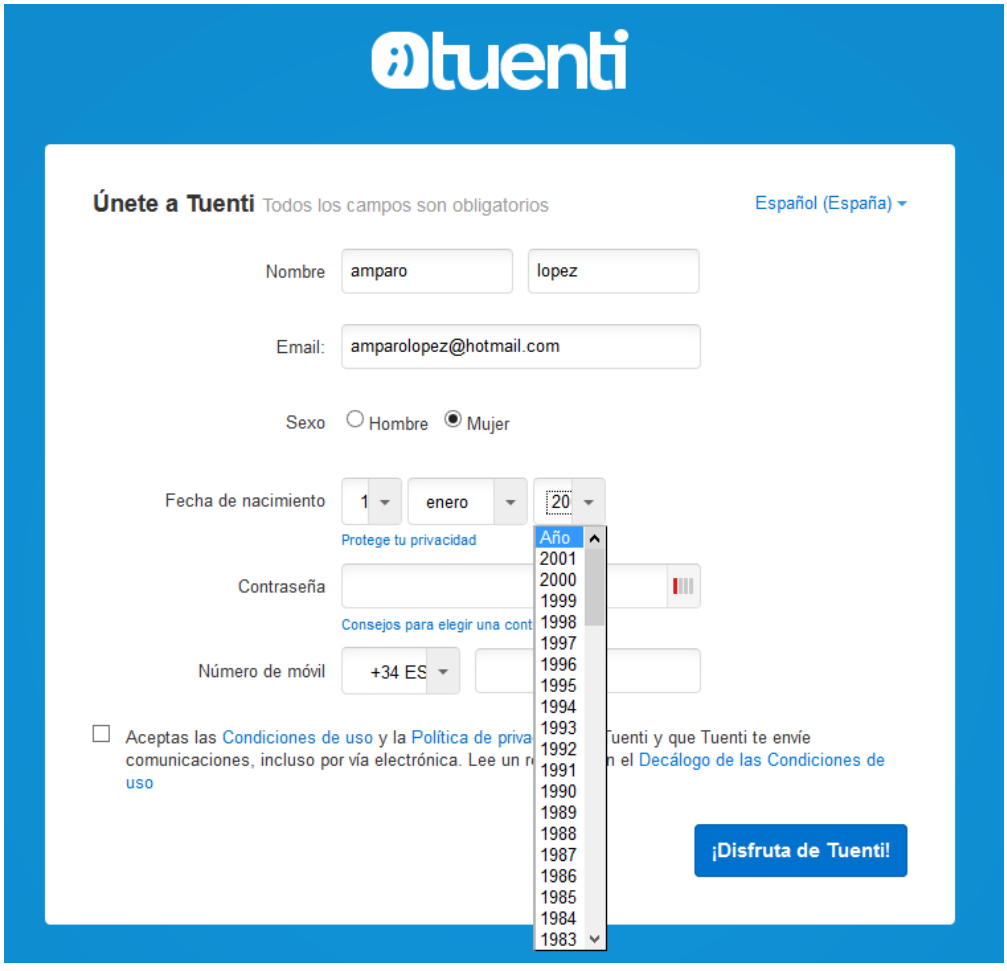
Uno de los riesgos que se han mencionado a lo largo de este documento era la posibilidad de crear cuentas falsas.

Para tratar de evitarlo, algunos proveedores como Tuenti, solicitan un número de teléfono para el alta al que se enviará un mensaje de confirmación para formalizar la cuenta del nuevo usuario registrado. A priori parece una medida bastante eficaz, pero hay que tener en cuenta que no se aplica de forma retroactiva a las cuentas preexistentes a la implantación de la misma.

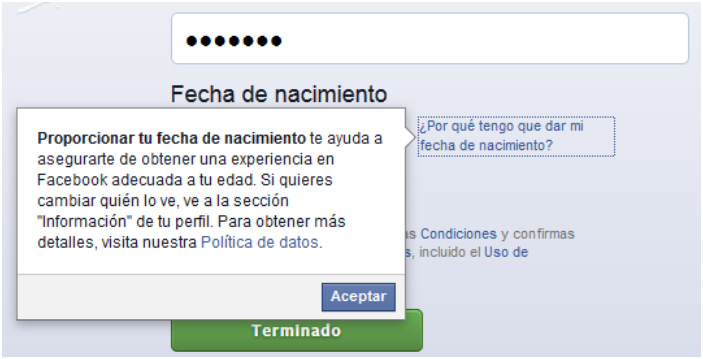
Como es sabido y se ha podido comprobar en la legislación aportada, los menores pueden requerir el permiso o autorización de sus padres o tutores legales para compartir algunos tipos de información y, recordemos, es obligación de los padres y tutores legales velar por la intimidad e imagen del menor (***Ley Orgánica 1/1982, de 5 de mayo***), por lo que la práctica totalidad de las redes sociales tienen requisito de edad para registrarse.

En España, la edad a partir de la cual los menores pueden usar las redes sociales es de 14 años, motivo por el cual, las redes como Facebook, Tuenti o Twitter no permiten el registro si se indica que se tiene una edad menor (Facebook, Twitter), o directamente no permite seleccionar fechas más recientes a la hora que determinar el año de nacimiento del solicitante (como Tuenti).

Fig.7 – Registro de Tuenti



En Facebook se solicita el año de nacimiento e indican que se hace para facilitar una experiencia adecuada a la edad:



Esto incluye no mostrar los datos de los menores tales como centro de estudios o fecha de nacimiento en las búsquedas de todos los usuarios, así como recordarles que deben limitar interacciones con desconocidos o con quien comparten contenidos, así como la aplicación por defecto de la "Revisión de Etiquetas" y de la "Revisión de Biografía", con las que pueden eliminar las etiquetas en las publicaciones o fotografías de otros usuarios antes de que estas aparezcan en sus perfiles.

Además, algunas redes sociales como *Facebook* utilizan algoritmos de detección de menores, aplicados a los comentarios, tanto emitidos como recibidos por el usuario y a las expresiones y modismos en ellos empleadas, así como el uso de *cookies* para el control de la identidad de los usuarios

Incluso se empiezan a barajar otras alternativas tales como la biometría aplicada a las fotos de los perfiles o escáneres de retina, aunque actualmente no se encuentran implantadas.

Para determinar el alcance de este problema, la propia *Facebook*, por boca de uno de sus directivos en Reino Unido se reconoce incapaz de impedir la presencia de menores en su red, al no contar con ningún mecanismo efectivo aplicable a esta problemática. Incluso han afirmado que los menores cuentan en muchos casos con la aquiescencia de sus padres para tener perfiles falsos y poder así hacer uso de la red social. [64]

Para evitar perfiles falsos, Facebook ha incorporado una validación de perfil en la creación de la cuenta, en la que se solicita un número de teléfono para comprobar la identidad de la persona en el momento del registro, o en su defecto una notificación

Otra de las medidas de control que poseen algunas redes sociales trata de localizar posibles amenazas a los menores comprobando los perfiles que se visitan de modo que, si un adulto visita con asiduidad muchos perfiles de menores, y/o emite a los mismos solicitudes de amistad tratando así de prevenir el *Grooming* mediante la creación de listas negras tanto de contenidos y páginas externas como de perfiles,

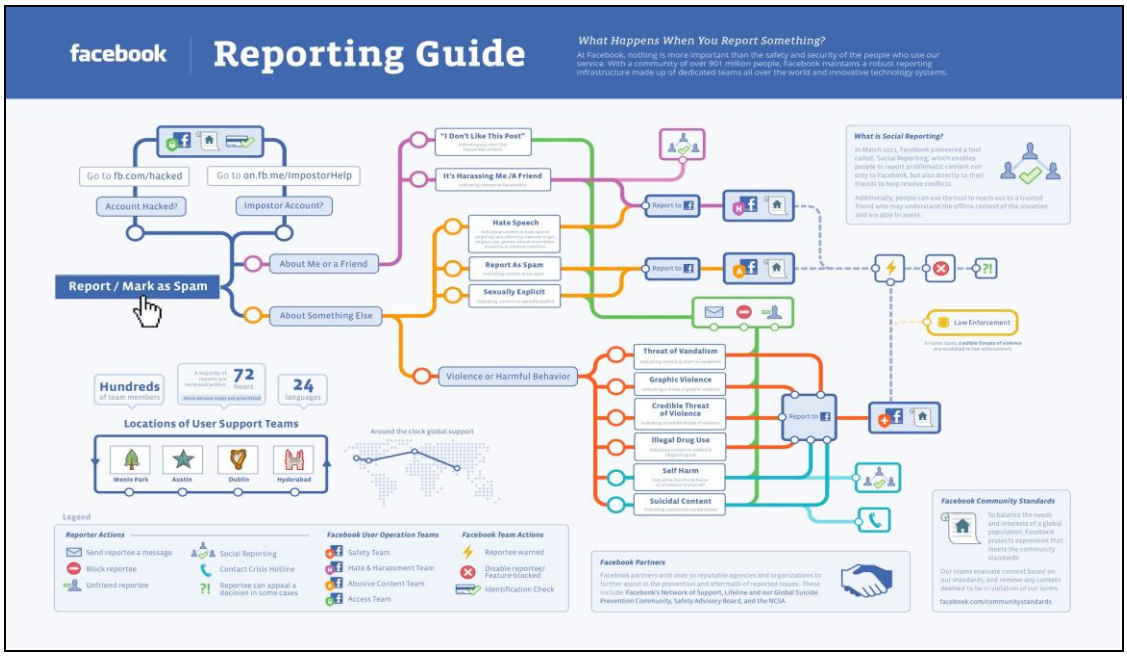
Estas mismas listas negras se emplean para luchar contra la pornografía, por ejemplo, mediante el uso de algoritmos que detectan y permiten bloquear mensajes, videos e imágenes de contenido sexual, aunque, como ya hemos explicado, en ocasiones no sean todo lo fiables que fuera deseable y se bloqueen fotos de lactantes, obras artísticas (como en caso del cuadro "El origen del Mundo") u otros. [67]

Otra de las acciones que las redes sociales llevan a cabo para prevenir el mal uso de las mismas es la opción de denunciar contenidos (videos, imágenes, comentarios…) que se puedan considerar inadecuados e incluso ilegales o delictivos, grupos, que ataquen a personas o fomenten la violencia o el uso de drogas, por ejemplo.

A este respecto, por ejemplo, existen en Facebook unas "Normas Comunitarias" en las que se incluyen los motivos por los que un grupo puede ser denunciado que van, como se ha mencionado, desde fomentar el consumo de drogas o la violencia, hasta infligir derechos de propiedad intelectual, de modo que cuando se recibe una denuncia, se revisa el contenido o el hecho denunciado respecto de un grupo o usuario y se toman las acciones oportunas, que pueden ir desde el bloqueo de la cuenta o grupo o la eliminación del contenido, a poner el hecho en conocimiento de las autoridades pertinentes.

En la siguiente figura se aporta un diagrama acerca del tratamiento de las denuncias recibidas en Facebook:

Fig.8 – Proceso de denuncia en Facebook



Otra de las medidas que las redes sociales permiten para evitar malos comportamientos, aunque parezca obvia, es la configuración de la privacidad de la cuenta de modo que se pueda elegir quién ve nuestros contenidos, publicaciones o nuestro correo electrónico o número de teléfono (p.ej. ahora *Facebook* permite registrarse con número de teléfono en lugar de e-mail, debido al uso masivo de la red con teléfonos Smart). Igualmente permite que elijamos quien puede enviarnos solicitudes de amistad e incluso si queremos ser localizados por buscadores externos (como *Google* o *Yahoo*).

A continuación mostramos las opciones de configuración de privacidad de *Tuenti* y *Facebook*:

Fig.9 – Opciones de privacidad en Tuenti

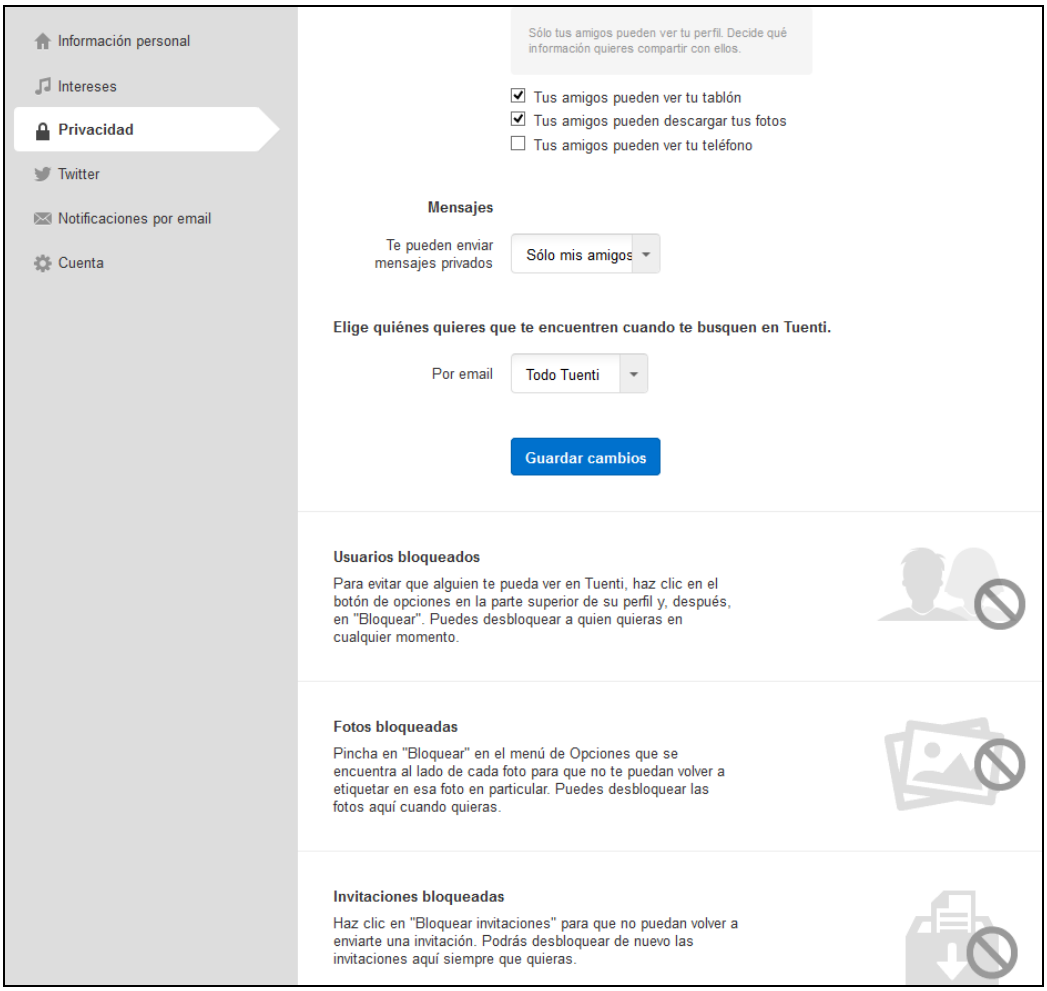


Fig. 10 – Opciones de privacidad en Facebook

Configuración y herramientas de privacidad

¿Quién puede ver mis cosas?	¿Quién puede ver las publicaciones que hagas a partir de ahora?	Amigos	Editar
	Revisa todas tus publicaciones y los contenidos en los que se te ha etiquetado		Usar registro de actividad
	¿Quieres limitar el público de las publicaciones que has compartido con los amigos de tus amigos o que has hecho públicas?		Limitar el público de publicaciones antiguas
¿Quién puede ponerse en contacto conmigo?	¿Quién puede enviarte solicitudes de amistad?	Todos	Editar
	¿De quién quiero filtrar los mensajes en mi bandeja de entrada?	Filtrado estricto	Editar
¿Quién puede buscarme?	¿Quién puede buscarte con la dirección de correo electrónico que has proporcionado?	Amigos	Editar
	¿Quién puede buscarte con el número de teléfono que has proporcionado?	Amigos	Editar
	¿Quieres que otros motores de búsqueda muestren el enlace de tu biografía?	No	Editar

En un ejercicio de transparencia, algo que se lleva demandando mucho tiempo a las redes sociales, se remiten de forma clara y detallada informaciones al usuario relativas a la seguridad, a la información que de los usuarios se recopila y con qué fines, durante cuánto tiempo se conservará...

Fig. 11. Política de datos de Facebook.

En el anexo 4 se encuentra recogida la Política de Datos de Facebook para su consulta.

Otra de las medidas adoptadas en lo referente a las transacciones comerciales es la adopción generalizada tanto de TPVs o Terminales de Punto de Venta (que son proporcionados por los bancos y entidades financieras con el fin de asegurar que las transacciones con tarjeta de crédito o débito que se realizan en Internet son seguras, y que el comprador no conoce ni almacena los datos relativos a la tarjeta empleada) como de protocolos de puerto seguro (SSL), lo que otorga una mayor seguridad a los usuarios ya que garantiza que los datos de la transacción no son accesibles a terceros, al encontrarse cifrados.

Igualmente se están implantando de forma exitosa y generalizada sistemas de identificación basados en firma digital, tanto en *sites* de comercio electrónico como en administraciones públicas, entre otros.

Mediante esta firma puede confirmarse la identidad de los interlocutores en la transacción comercial o administrativa, así como confirmar el consentimiento prestado a la misma, lo que otorga seguridad en la transacción no sólo al cliente, sino al operador, al poder establecerse un mecanismo de "no repudio" a través de los datos recopilados en la mencionada transacción.

Además de las mencionadas, cada día los proveedores de servicios de las redes sociales online tratan de que éstas sean entornos lo más seguros posibles y para que nuestra experiencia como usuarios sea lo más placentera posible.

CAPÍTULO 5

RECOMENDACIONES Y CONSEJOS

5.1 Recomendaciones para los usuarios de redes sociales online

Como ya se ha visto, las propias plataformas de las redes sociales tratan de mejorar cada día para ser lo más seguras posibles y de darnos los mejores medios para poder usarlas de modo adecuado.

Pues bien, a pesar de ello, debemos tener muy claro que la responsabilidad última de lo que hacemos con nuestros datos, con nuestra información, en definitiva, con nuestra ***vida virtual***, es nuestra.

Debemos adoptar una postura de usuarios y consumidores responsables y aprovechar las maravillosas oportunidades que las redes sociales online nos brindan de forma consciente y segura.

A continuación pasaremos a detallar una lista de recomendaciones para hacer un uso adecuado de las redes sociales online que nos permita usarlas de un modo lo más seguro posible.

1- ***Aprender el manejo de la red empleada y de la configuración de privacidad:***

Como si de un electrodoméstico se tratase, es conveniente conocer el manejo de la red social y para ello nada mejor que una lectura de las "instrucciones de uso". Debemos conocer las redes que empleamos, pero no solo en lo más elemental como agregar contactos, enviar mensajes o compartir contenidos, sino que es conveniente conocer las opciones de privacidad para configurarlas según nuestro gusto y necesidades

Incluso la AEPD se hace eco de esta recomendación para no aceptar sin más las configuraciones por defecto para móviles y redes sociales en lo tocante a la privacidad. Según un estudio que manejaba la propia AEPD en 2014, el 76% de

los españoles estaban preocupados por la protección de los datos personales y el posible uso de esa información por parte de terceros. [68]

Es conveniente también, estar al tanto de las modificaciones en lo tocante a la privacidad de las propias redes sociales ya que éstas están en constante evolución y, aunque generalmente los cambios son "a mejor", es decir, que mejoran la privacidad (como por ejemplo Facebook que en Mayo de 2014 cambió las opciones por defecto para que los "posteos" realizados sólo fueran vistos por los amigos del usuario), es conveniente conocerlos para evitar sorpresas desagradables. [69]

2- Leer toda la información relativa a la red social:

Aunque todos sabemos que una de las asignaturas pendientes de las redes sociales es redactar los acuerdos de licencia de uso (EULA, en inglés) de forma clara y fácilmente comprensible por la mayor parte de los usuarios, debemos intentar comprender los términos del contrato que estamos aceptando para evitar sustos posteriores.

Como ya hemos comentado anteriormente, el tan extendido uso del "siguiente, siguiente" en las instalaciones de software y aceptación de condiciones de uso en internet es una fuente de riesgos bastante importante.

3- Utilizar distintos nombres de usuario y contraseñas:

No es conveniente utilizar los mismos nombres de usuarios y contraseñas para las diversas redes a las que un usuario pueda acceder ya que esto dificulta los ataques y el riesgo de ser suplantado en ellas, teniendo que vulnerar la seguridad en los distintos sistemas de acceso en lugar de bastarles con uno sólo.

4- Uso adecuado de contraseñas:

Se recomienda el uso de contraseñas robustas, de una longitud mínima de caracteres, que contengan mayúsculas y minúsculas, así como números y caracteres especiales.

Así mismo se recomienda que se cambien periódicamente y que no sean fácilmente detectables por "ingeniería social", esto es, descartar el nombre de mascotas, hijos, grupos de música favoritos, etc.

Hay que ser cuidadoso con las contraseñas almacenadas en el navegador, ya que pueden hacernos vulnerables ante un acceso al mismo.

5- Mantener actualizados el navegador y el sistema operativo:

Para evitar amenazas es aconsejable mantener actualizados tanto el navegador de internet como el sistema operativo, utilizando software legal, ya que ofrece garantía y soporte.

También se aconseja una adecuada configuración del navegador para que sea seguro y estar muy atento a las novedades y alertas de seguridad.

6- Emplea analizadores de enlaces:

Pueden emplearse analizadores de enlaces para saber si la URL a la que vamos a conectarnos enlaza una página segura o por el contrario, lo hace a una maliciosa.

7- Empleo de antivirus:

Se recomienda el uso de software antivirus, antimalware (spyware) y firewalls, y que se encuentre convenientemente actualizado para evitar virus o aplicaciones de spyware (*troyanos, keyloggers*…) que puedan comprometer los datos e informaciones almacenadas en sus equipos o publicadas en las redes sociales.

8- Descargar sólo de páginas oficiales:

Se aconseja descargar las aplicaciones de páginas oficiales para evitar suplantaciones así como analizar todas las descargas con el antivirus.

9- Desconfiar de mensajes y correos de remitentes desconocidos:

Hay que desconfiar de este tipo de mensajes y eliminarlos ante el menor atisbo de duda.

Por supuesto, esto incluye no descargar ningún archivo adjunto que el mencionado mensaje pudiera llevar.

Como ejemplo, este mismo año, la Policía Nacional alertó de un caso de spam, en el que se recibía un email fraudulento de Correos en el que se indicaba que se había recibido un paquete, pero al seleccionar el enlace de la notificación, se descargaba un *malware* que cifraba todos los datos del ordenador, solicitando una elevada cantidad económica para su descifrado. [70]

Fig. 12. Ciberataque mediante suplantación

10- Cuidado con la difusión de nuestro email y cuentas de las redes sociales

No se deben facilitar a la ligera nuestras cuentas de correo de las RRSSO para controlar quien tiene acceso a las mismas.

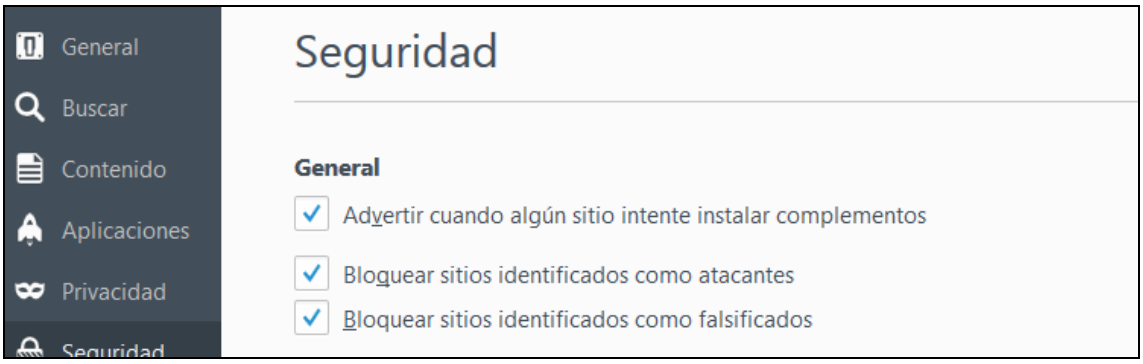
11- Cuidado con las conexiones seguras:

Hay que cuidar que las conexiones seguras (aquellas en las que la información viaja cifrada) se corresponden con URLs que comiencen por "*https://*" en nuestro navegador. En ellas se cifra la información mediante un intercambio de claves públicas y que hacen que sólo pueda descifrarse haciendo uso de una clave privada.

Para evitar el ***pharming*** y el ***phising***, ya descritos en el Capítulo 4, hay una serie de consejos que también son aplicables:

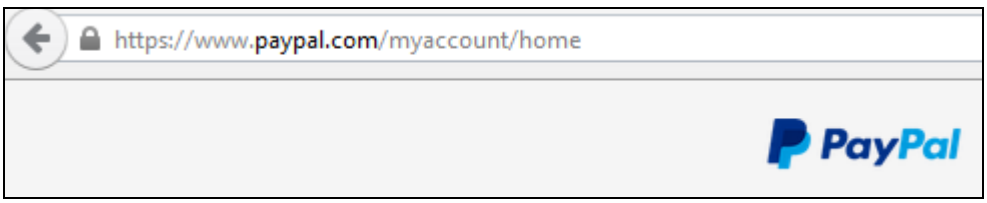
- Configurar nuestro navegador correctamente para prevenir este tipo de ataques.

Fig. 13. Configuración antiphishing del navegador



- Revisar la barra de direcciones de nuestro navegador y ver que comienza por *https://*.
- Revisar si en nuestro navegador aparece un icono de un candado cerrado tal y como se muestra en la siguiente figura

Fig. 14. Comprobación de conexión segura.



12- Verifica los correos entrantes:

Las entidades bancarias nunca solicitan claves o datos personales por correo. Ante la duda, se debe acudir a la oficina bancaria o llamar por teléfono.

De igual modo, los entes públicos tales como ministerios, Seguridad Social o Agencia Tributaria tampoco nos solicitarán información delicada por email, por lo que es aconsejable contactar por teléfono o concertar una cita en caso de duda.

Los correos de *phishing* frecuentemente no se dirigen a nosotros personalmente, sino mediante saludos genéricos ("Estimado cliente", "Estimado usuario").

Ocasionalmente también se pueden localizar faltas ortográficas o gramaticales, ya que suelen emplearse traductores automáticos para generar estos mensajes y enviarlos masivamente.

No debemos dejarnos apremiar por estos correos, ya que pueden inducirnos una sensación de urgencia con mensajes como "Su cuenta está en riesgo", "Actualice urgentemente", e incluso tentándonos con premios.

13- Nunca entrar en webs bancarias mediante links:

No se debe entrar en las webs de las entidades bancarias o de transacciones económicas (Paypal, etc) mediante links ya que es preferible acceder insertando la dirección adecuada en la barra de direcciones del navegador.

En todo caso, se deben revisar los vínculos, ya que muchos correos electrónicos de phishing incluyen un vínculo que parece válido, pero que puede enviar a un sitio fraudulento.

Se debe comprobar siempre el vínculo antes de pulsarlo. Se puede mover el ratón por encima del enlace y ver la URL del navegador (en la figura de abajo puede verse en la parte inferior izquierda).

Fig. 15. Consejo antiphising.

No se debe emplear el vínculo en caso de ser sospechoso.

A modo de ejemplo, en Febrero de 2015, se cerraron varias webs que simulaban ser PayPal y que se enviaban mediante correos que contenían links a las mismas. [71]

14- No publicar datos excesivos:

No se recomienda aportar excesivos datos personales si no se tiene clara la finalidad con la que se aportan o si no se hace para alguna finalidad específica.

Las redes sociales habitualmente tratan de recopilar una gran cantidad de datos para definir perfiles de usuarios lo más detallados posibles, pero esta posibilidad puede no ser deseada por nosotros.

Siempre hay que pensar en primera instancia si queremos compartir ese tipo de información. Por ejemplo, si me he registrado en una red social para contactar con antiguos compañeros del colegio, puede que indicar donde trabajo o mis inclinaciones políticas o religiosas no sea necesario.

15 -Ser conscientes de la difusión de las redes online:

Hay que entender que las redes sociales online son ventanas abiertas y que cualquier cosa que se publique, por inocente que pueda parecer puede tener un largo recorrido.

A modo de ejemplo deberíamos pensar si publicar cuándo y dónde se va a encontrar alguien de vacaciones puede ser contraproducente (podría facilitar algún robo en su residencia habitual, por ejemplo).

16- Ser consciente de la perdurabilidad de los datos en las RRSSO:

Hay que tener en cuenta que los contenidos que compartimos en las redes sociales pueden estar activos y/o accesibles mucho más tiempo del que deseamos.

En España ha sido muy comentado el caso de un concejal madrileño que difundió unos chistes de mal gusto hace varios años en twitter y que ha tenido que dimitir a causa de los mismos.

Es aconsejable que pensemos bien en los contenidos que compartimos y que estos sean respetuosos dado que podrán estar accesibles largo tiempo.

Igualmente, se aconseja revisar cada cierto tiempo nuestras cuentas de las redes sociales si creemos que debemos eliminar, corregir o matizar alguno de los mismos.

17- Ser respetuoso con la información:

Hay que ser respetuoso con la información ajena y preguntarnos si a alguien le gustaría que publicásemos esta o aquella foto o diésemos algún recorrido a un video o comentario suyo.

Es aconsejable comentar siempre con nuestros contactos antes de difundir este tipo de informaciones, especialmente si pueden involucrar a menores tales como hijos, familiares…

Del mismo modo, debemos exigir a nuestros contactos que sean lo más cuidadosos posibles con la difusión de nuestros datos e informaciones, especialmente los personales, así como el tratamiento de nuestra imagen pública, y hacerles saber si nos gustaría ser consultados y en qué casos.

18- Respetar la propiedad intelectual e industrial:

Hay que tener en cuenta que los creadores, pero también el resto de usuarios de la red, y las personas fuera de esta, tienen determinados derechos sobre sus creaciones intelectuales y que no pueden difundirse de forma pública sin la autorización expresa de los mismos.

Esto que a priori puede parecer un asunto menor, puede conllevar fuertes sanciones económicas e incluso penales.

19- Tener cuidado con el uso de webcams:

Es conveniente tener cuidado con el uso de webcams, especialmente en smartphones, tabletas y ordenadores portátiles en los que viene preinstalada ya que solemos olvidarnos de la misma.

Un hacker malintencionado puede hacerse con el control de la cámara y tomar imágenes de la intimidad de las personas para tratar de coaccionarlas, chantajearlas o con algún otro fin ilegítimo.

Es conveniente activar la webcam sólo cuando se necesite, e incluso puede ser aconsejable tapar la misma cuando no se use con un adhesivo o similar.

Se debe enseñar a los menores a dar un uso correcto de estos aparatos y los riesgos derivados de compartir fotografías o vídeos.

20- Evitar riesgos de geoetiquetado:

Aunque, como ya se ha indicado, la mayor parte de las RRSSO eliminan de forma automática las marcas de geoetiquetado, no está de más desactivarlo de nuestros dispositivos (smartphones, tabletas…).

Para ello basta con ir a la aplicación de captura de imágenes de nuestro dispositivo (cámara) y revisar las opciones de configuración, desactivando aquellas relativas a *Geoetiquetado*, *Ubicación*, *Etiqueta GPS*… que variarán dependiendo del fabricante.

Un ejemplo para un dispositivo *Android*:

Fig. 16. Geoetiquetado en dispositivo Android

21- Cuidar nuestra conexión a internet:

Al igual que hemos hablado de la necesidad de elegir claves robustas y de cambiarlas con asiduidad, es aconsejable hacer lo propio con la de nuestro *router* de casa o de la oficina, especialmente si es inalámbrico (*Wifi*), para evitar intrusiones en nuestra red que pongan en riesgo nuestra información. Es importantísimo cambiar siempre las claves por defecto del *router*, así como de cualquier dispositivo que empleemos para conectarnos a Internet o las redes sociales.

Del mismo modo, es aconsejable ser prudente con el uso de redes abiertas y públicas, y sólo usarlas si son de total confianza, por ejemplo, podría no ser aconsejable realizar compras, transacciones bancarias o gestiones administrativas en alguna de estas redes.

22- Mantenerse informado sobre las novedades relativas a la seguridad:

Es recomendable que estemos al tanto de las noticias sobre vulnerabilidades relativas a nuestros modelos tanto de software (Sistema operativo, navegador, antivirus…) como hardware (sobre todo *routers*) para anticiparnos a situaciones como la descrita en las siguientes noticias [72]:

SEGURIDAD | NOTICIAS | 08 JUN 2015

Un estudio español descubre 60 vulnerabilidades en 22 modelos de routers

Tags: Seguridad Estudios

También te puede interesar:

- ¿Cómo será tu próximo router?
- Más de 700 mil routers expuestos a ataques

Un grupo de investigadores de seguridad españoles ha descubierto 60 vulnerabilidades en 22 modelos de routers de diferentes fabricantes, que son distribuidos en su mayoría por los propios proveedores de servicios de Internet a los clientes.

MÓVILES

Dos fallos de seguridad ponen en riesgo a casi 2.000 millones de «smartphones»

ABC TECNOLOGÍA / MADRID | Día 04/08/2014 - 09.03h

23- Hablar con los menores acerca de los peligros de las redes sociales e Internet:

Aunque no hay porqué alarmarles, es conveniente que los menores entiendan qué información pueden compartir y cual no, qué personas pueden agregar como contactos, amigos o *followers* y qué peticiones deben rechazar.

Así mismo deben entender que su imagen es importante y valiosa y que deben ser prudentes y educados tanto en sus comentarios como en todos aquellos contenidos que compartan.

Deben entender que su "yo virtual" no es sino una extensión de su persona física y que cualquier acto en las redes sociales puede tener repercusión en su vida real, y viceversa.

Además, también es importante que entiendan por qué no pueden registrarse en alguna red social hasta una edad determinada o por qué insistimos en que nos agreguen como amigos o contactos.

24- Ser seguidores de la actividad de nuestros hijos en las redes sociales:

Es importante que sepamos qué hacen nuestros hijos en las redes sociales: a quién siguen, quienes son sus contactos, e incluso a qué horas se conectan.

Esto puede conseguirse de varios modos, ya sea haciéndonos "amigos" de nuestros hijos en las redes sociales o, por ejemplo, mediante el uso de programas

de control parental, para conocer la actividad online que nuestros hijos desarrollan: qué sitios web visitan, cuando lo hacen...

25- Hacer un uso racional de las redes sociales:

Es conveniente que pongamos unos horarios a los menores sobre el uso de las redes sociales, ya que como se ha comentado pueden llegar a ser fuertemente adictivas, especialmente aquellas que disponen de aplicaciones propias y plataformas de juegos.

Aunque se acaba de hacer referencia expresa a los menores, también es aconsejable que este control horario se auto-imponga por parte de los adultos, ya que tampoco estos se encuentran exentos de los riesgos de un uso excesivo de las redes sociales.

26- Poner el ordenador en un lugar común de la casa:

Puede ser útil, sobre todo para el recién comentado control de horarios, que el punto de acceso a Internet y las redes sociales se encuentre en un lugar común de la casa, siempre fuera del dormitorio de los menores, para asegurarnos de cuando accede el menor y a qué contenidos.

Hay que tener en cuenta que este punto de acceso no es solo un PC de sobremesa como ocurría hace algunos, sino que incluye tabletas, portátiles, smartphones…

En este punto, incluso puede ser conveniente determinar si el menor necesita un dispositivo determinado (un Smartphone, por ejemplo) u otro (un teléfono convencional) según el uso que queramos que de al mismo.

27- Acompañar al menor:

Se aconseja acompañar al menor tanto en la navegación en Internet como en el juego como un partícipe más.

En tanto que el menor no nos perciba como un elemento controlador, aumentará su confianza en nosotros de modo que mejorará su comunicación sobre lo que hace dentro de la red y nos permitirá anticiparnos a situaciones complicadas.

28- Hacer uso de los mecanismos de denuncia:

Cuando se detecte un uso indebido de las redes sociales o seamos víctimas del mismo debe denunciarse lo antes posible, ya sea al proveedor del servicio o, si la gravedad del caso lo requiriese, ante las autoridades pertinentes.

Debemos indicar a los menores que nos informen ante cualquier abuso o situación peligrosa sufrida, así como a sus profesores u otros adultos indicados.

29- Usar bloqueadores de contenidos:

Puede ser útil hacer uso e bloqueadores de contenidos para asegurarnos que aquellos contenidos que no consideramos aptos para los menores no puedan ser visitados por estos.

30- Concienciar sobre los encuentros en vivo:

Hay que enseñar a los menores que nunca han de quedar en el mundo real con alguien al que sólo se ha conocido por internet o una red social y que, si lo hacen, deben ir acompañados por sus padres o tutores para evitar posibles peligros.

31- Revisar con asiduidad los perfiles de los menores a nuestro cargo:

Es conveniente revisar de forma periódica qué tipo de información comparte el menor y que datos pone a disposición de otros.

32- No usar el nombre completo:

Puede ser aconsejable para los menores no hacer uso de su nombre completo en las redes sociales, o incluso hacer uso de un pseudónimo para dificultar ser identificables por terceros malintencionados.

33- Dialogar con los menores:

Como ya se ha indicado con anterioridad, las redes sociales no son sino un aspecto más de la vida real, por lo que mantener una actitud receptiva y dialogante con los menores, tanto para explicarles la realidad de las redes sociales como para escuchar sus apreciaciones, experiencias o demandas es la base para un uso satisfactorio de las mismas, para anticipar la mayor parte de las amenazas, así como para atajar las situaciones indeseables de forma rápida y eficaz una vez que surgen.

5.2 Recomendaciones para las empresas y proveedores de servicios

Como ya se ha mencionado con anterioridad, los proveedores de servicios sufren ataques y también hay una serie de recomendaciones para los responsables de seguridad y los auditores de los sistemas que pueden permitir evitar algunos problemas.

A continuación daremos algunas indicaciones que podrían ser útiles:

1- Cumplir la ley:

Esta recomendación que parece una perogrullada no siempre se cumple. Se han dado casos de empresas que han cedido datos a terceros sin la autorización expresa de los clientes, de empresas que no han procedido al borrado de datos de clientes que lo solicitaron de forma expresa al dejar de serlo, envío de facturas a personas ajenas al servicio…

En ocasiones estas situaciones responden a incidencias o problemas en el sistema sin intencionalidad alguna y, en esos casos, se debe tener el máximo celo tanto para evitarlas como para solucionarlas rápida y eficazmente.

Más preocupantes son aquellas situaciones en las que sí hay intencionalidad por parte de la empresa con fines, si no delictivos, al menos claramente lucrativos.

Algunas noticias del mundo empresarial al respecto [73]:

Groupon sancionada por no informar que almacenaba los datos de las tarjetas de crédito de sus clientes

Publicado por: Samuel Parra el 14 de febrero de 2014 9 Comentarios

ONO sancionada por ceder datos de clientes a guías y buscadores de Internet

Las eléctricas entre las compañías más sancionadas por la AEPD

Por fran 31 marzo, 2015 Comentarios desactivados en Las eléctricas entre las compañías más sancionadas por la AEPD

Durante 2014, **los nombres de grandes empresas eléctricas como Galp, Endesa, Gas Natura, Iberdrola e Hidrocantábrico fueron muy recurrentes en las sanciones impuestas por la Agencia Española de Protección de Datos.**

Tres fueron los motivos principales de este hecho:

- usar datos personales de los clientes para cambiarles de suministrador eléctrico sin su consentimiento
- añadir a usuarios en listas de morosos sin justificación para ello
- y enviarles facturas a usuarios a los que no les unía ninguna relación

2- Tener claro que datos son personales y cuales no:

Lo primero que se debe tener en cuenta es que tipo de información se está manejando, si es sensible o no, si debe tener cierto grado de protección u otro mayor…

No siempre en el mundo de la empresa se tiene en cuenta una adecuada clasificación de datos que permita asegurar tanto la integridad de los mismos como su correcta clasificación, de modo tal que en bases de datos se cruzan tablas con datos personales y otros que no lo son. En otros casos se emplean claves ajenas indebidas (frecuentemente NIF, CIF…) o incluso se exportan datos reales a entornos no productivos (desarrollo, pruebas, integración…) con el agravante de que los niveles de seguridad en estos entornos pueden diferir de los entornos productivos.

De esta adecuada disociación de los datos se obtiene una ventaja incluso mayor y es que, ante un acceso indebido a los mismos pueden protegerse mejor determinados datos relativos a los perfiles de los usuarios afectados.

Un dato curioso es que la AEPD considera la IP de los usuarios de Internet como un dato de carácter personal e igualmente lo considera el Tribunal Supremo que lo incardina dentro de los contemplados en el artículo 3.a de la LOPD en reciente sentencia [74]:

22/10/2014 09:10:00 | REDACCIÓN NJ | PROTECCIÓN DE DATOS

Las direcciones IP de los usuarios de Internet deben ser consideradas como datos personales y por tanto, están protegidos por la LOPD

La Sección Sexta de la Sala de lo contencioso-administrativo del Tribunal Supremo ha dictado una sentencia de fecha 3 de octubre de 2014 (recurso número 6153/2011), por la que establece una interesante doctrina sobre la consideración de la claves IP, a efectos de la protección de datos de carácter personal.

La sentencia estima, con base en la STJUE de sentencia de 24 de noviembre de 2011 (asuntos acumulados C-468/10 y C-469/10, caso ASNEF), que **las direcciones IP son datos personales, en el sentido del artículo 3.a) LOPD y, como tales, se encuentran protegidos por las garantías establecidas por dicho texto legal para su tratamiento.**

Al no producirse la imposibilidad de informar a los intersados del tratamiento de sus direcciones IP, ni exigir dicho trámite un esfuerzo desproporcionado al obligado al mismo, no concurren los motivos exigidos para aplicar la exención del deber de informar al interesado del tratamiento de sus datos.

3- Generación de perfiles de usuarios:

Es necesario que los permisos que los usuarios tienen en el sistema (especialmente empleados) tengan únicamente aquellos privilegios indispensables para el desempeño de sus funciones.

4- Usuarios personales:

Es aconsejable evitar en la medida de lo posible el uso y existencia de usuarios genéricos ya que dificultan la monitorización de acciones de una persona dentro del sistema.

5- Establecer políticas obligatorias de seguridad:

En este punto se incluyen reseteos obligatorios de claves, que no permitan usar las ya empleadas y que exijan unas diferencias mínimas entre ellas, así como una longitud y complejidad determinadas para evitar que puedan ser fácilmente detectadas por terceros.

6- Mantener un control de accesos al sistema:

Es recomendable mantener un control del acceso de los usuarios al sistema y que se recoja la máxima información posible: login, horas de acceso, IPs, acciones o transacciones efectuadas.

Así mismo es aconsejable mantener un histórico de esta información para posteriores comprobaciones si fuera necesario.

7- Generación de ficheros de log:

Se recomienda mantener logs de los procesos que permitan su estudio en caso de incidencia o fallo de seguridad.

8- Determinar rangos de validez de datos:

Como ya hemos indicado en el caso de la Inyección SQL, es aconsejable que los datos se definan con unos rangos realistas y adecuados tanto para los datos que van a almacenar como para su procesamiento.

9- Aplicar diálogos de control interactivos:

En este caso se podrán prevenir ataques con *bots* y similares.

10- Controlar la presencia de anomalías de datos:

Si los datos están debidamente definidos, estas anomalías podrían indicar que han sufrido algún tipo de manipulación o tratamiento posterior.

11- Proteger los datos adecuadamente:

Es muy aconsejable el cifrado de los datos para evitar su difusión en caso de acceso indebido a los mismos, así como eliminar aquellos que sean obsoletos lo que incluso podría suponer mejoras en el rendimiento de las plataformas y ahorro de costes.

Además de las indicadas, otras acciones pueden ser muy beneficiosas para prevenir acciones no autorizadas sobre los datos, tales como limitar los datos a un área geográfica determinada o a algunos perfiles específicos.

12- No recoger más datos de los necesarios:

Tal y como se recoge en la LORTAD, los datos que se recojan deben ser acordes a la finalidad con la que se recogen. Tomar sólo los datos imprescindibles nos evitará problemas en la gestión de los mismos, incluso abaratando costes de recopilación y/o almacenamiento. Además, la toma indiscriminada de datos puede tener otro tipo de consecuencias tal y como ha ocurrido recientemente con la aplicación Spotify, ideada originalmente para escuchar música online y que recientemente ha cambiado su política de privacidad, lo que le ha causado numerosas críticas (¿para qué necesita acceder a mis fotos o contactos de Facebook una aplicación de reproducción de música?) así como un importante descenso de usuarios [75]:

Spotify pide disculpas por sus cambios en la política de privacidad

- Los cambios en sus normas soliviantaron a la comunidad
- Spotify emitirá vídeos para competir con YouTube

R. J. C. | San Francisco | 22 AGO 2015 - 11:20 CEST

Si revisamos estas indicaciones, parecen todas de sentido común, pero resultan inconexas y faltas de rigor por lo que, a continuación, propondremos un método operativo para las entidades profesionales que prestan los servicios online.

5.3 Solución propuesta para las empresas prestadoras de servicios: Norma ISO 27001

En lo referente a las entidades profesionales deben adoptarse protocolos y líneas de actuación claras y definidas, como las que se detallarán a continuación sobre el tratamiento de las normas ISO 27001 y 27002.

Si bien es cierto que el comportamiento y las exigencias de los usuarios en lo relativo al uso de las RRSSO no parece indicar que una certificación en esta norma pueda suponer un hándicap severo para aquellas entidades que no la posean, si puede considerarse un valor añadido o una ventaja competitiva estar en posesión de la misma para determinados colectivos profesionales, e incluso potenciales inversores.

Cabe mencionar, que recientes estudios catalogan la seguridad como un valor determinante para los usuarios en lo que a confianza se refiere sobre las marca digitales. Un 63% de los encuestados manifestaban desconfiar de marcas que habían sufrido ataques en el último año. [76]

La norma ISO/IEC 27001 es un elemento sobre el que basar la gestión y protección de la información de cualquier empresa, un Sistema de Gestión de la Seguridad de la Información (SGSI), que supone la un modo práctico para adoptar un conjunto de buenas prácticas que garanticen el tratamiento correcto de la información.

5.3.1 Beneficios

Algunos de los beneficios resultantes de la implantación de esta norma son:

- **Ayuda al cumplimiento de leyes y normativas**, tales como la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE), Propiedad Intelectual, etc.
- **Aporta un valor añadido**, dando a nuestros clientes una mayor credibilidad, ya que contar con esta certificación, asegura que tenemos un proceso adecuado para la gestión de la información.
- Ofrece una **metodología** para llevar a cabo un Análisis y Gestión de Riesgos.
- **Garantiza la implantación de medidas de seguridad consistentes**, eficientes y apropiadas al valor de la información protegida.
- **Contempla planes de contingencia** ante cualquier tipo de incidencia (pérdidas de datos, incendio, robo, terrorismo, etc.)
- **Puede ser utilizada como herramienta de diferenciación** frente a la competencia.
- **Mejora la concienciación del personal** en todo lo que se refiere a la seguridad y a sus responsabilidades dentro de la organización.

Como ya hemos indicado con anterioridad, el auge de las nuevas tecnologías supone que el tratamiento de la información haya dado un cambio importante en la cultura empresarial y obliga a extremar las precauciones para garantizar algunos aspectos que ya recogimos en el tratamiento de la LOPD:

- La **confidencialidad**: Evitar que la información esté a disposición de individuos, entidades o procesos que no tienen autorización.
- La **disponibilidad**: Asegurar que la información sea accesible cuando sea necesario.
- La **integridad**: Mantener la información exacta y completa.

Contar con un SGSI nos permitirá determinar qué políticas y objetivos de seguridad deben ser implantados y nos ayudará a crear los mecanismos necesarios para proteger la información y los sistemas que los procesan.

5.3.2 Ciclo de vida de la norma

Para implementar un SGSI conforme a la norma ISO 27001 hay que establecer un ciclo 'Plan Do Check Act' (PDCA) como el utilizado en los sistemas de calidad:

- **Planificar (Plan)**:

  Establecer el SGSI, su alcance y objetivos. En esta fase deberá definirse la política de seguridad de la organización y la metodología para la evaluación de los riesgos que utilizaremos en nuestro Sistema. Posteriormente, deben identificarse los riesgos, evaluando las amenazas y vulnerabilidades que estos pudieran tener y el posible impacto en el negocio.

Una vez analizados los riesgos y determinadas qué situaciones no son aceptables para la empresa, se establecerá un plan para tratar y mitigar los riesgos no aceptables. Para ello, se aplicarán los controles oportunos. Deberán seleccionarse los objetivos de control y controles del anexo A de la norma ISO 27001 que serán utilizados para el tratamiento de los riesgos y serán recogidos en una declaración de aplicabilidad.

- **Hacer (Do)**:

  En esta fase se establece un plan para la gestión de los riesgos que incluya su oportuna planificación y desglose de responsabilidades y organización de los proyectos, así como la definición de una serie de indicadores que permitan conocer la eficacia y eficiencia de las acciones llevadas a cabo para la mitigación de los riesgos.

Se concienciará y formará a todos las personas y se implantarán los controles establecidos en la fase anterior.

- **Comprobar (Check)**:

  En esta fase se revisará la efectividad del sistema adoptado, así como los noveles de riesgo, especialmente cuando existan cambios en la organización, la tecnología, los procesos, etc…

El sistema deberá someterse a auditorías internas recurrentes y planificadas y el resultado de estas deberá ser revisada por el área responsable o la dirección de la empresa.

- **Actuar (Act)**:

  A partir de los resultados de los pasos anteriores, se deben adoptar las acciones necesarias para mejorar y afianzar el SGSI, alcanzando de este modo los objetivos planteados.

En este sentido, la ISO 27002 es una guía de buenas prácticas en la que se recogen recomendaciones sobre los aspectos indicados en los controles del anexo A de la ISO 27001, donde se habla de estos controles, pero sin detallarlos, ya que no debemos olvidar que la ISO 27001 define como gestionar la seguridad (como implementar un Sistema de Gestión de Seguridad de la Información).

5.3.3 Contenido

La ISO 27002 se emplea por tanto como una ayuda para gestionar debidamente los riesgos:

- **Política de Seguridad**. El objetivo de este control es contar con una Política de Seguridad documentada y revisada periódicamente.

  En este apartado se recogen las directrices en seguridad de la información.

  1. Conjunto de políticas para la seguridad de la información.
  2. Revisión de las políticas para la seguridad de la información.

- **Aspectos organizativos**. Este control establece cómo debería estar compuesta la organización de la seguridad de la empresa, cómo deben coordinarse las actividades y cómo deben mantenerse activas las relaciones con los terceros que pudieran colaborar con nosotros.

  En este apartado se recogen aspectos tales como:

  a) Organización interna.

  1. Asignación de responsabilidades para la seguridad de la información.
  2. Segregación de tareas.
  3. Contacto con las autoridades.
  4. Contacto con grupos de interés especial.
  5. Seguridad de la información en la gestión de proyectos.

  b) Dispositivos para movilidad y teletrabajo.

  1. Política de uso de dispositivos para movilidad.
  2. Teletrabajo.

- **Recursos humanos**. Dividido en tres controles, establece las medidas de seguridad que deberían considerarse en cada una de las fases de desempeño de trabajo (definición del puesto, desempeño de las funciones y a la finalización o cambio del puesto de trabajo).

  a) **Antes de la contratación.**

  1. Investigación de antecedentes.
  2. Términos y condiciones de contratación.

  b) **Durante la contratación.**

  1. Responsabilidades de gestión.
  2. Concienciación, educación y capacitación en Seguridad de la Información.
  3. Proceso disciplinario.

c) **Cese o cambio de puesto de trabajo.**

1. Cese o cambio de puesto de trabajo.

- **Gestión de activos**. Este apartado propone contar con un inventario detallado de activos que recoja sus funcionalidades. Además, establece pautas para el uso responsable y adecuado de los mismos. Este apartado recoge además la necesidad de contar con un procedimiento de tratamiento de la clasificación, así como las medidas de seguridad que deberían considerarse en función de la clasificación de estos.

a) Responsabilidad sobre los activos.

1. Inventario de activos.
2. Propiedad de los activos.
3. Uso aceptable de los activos.
4. Devolución de activos.

b) Clasificación de la información.

2. Directrices de clasificación.
3. Etiquetado y manipulado de la información.
4. Manipulación de activos.

c) Manejo de los soportes de almacenamiento.

1. Gestión de soportes extraíbles.
2. Eliminación de soportes.
3. Soportes físicos en tránsito.

- **Control de accesos.** Este apartado presenta las pautas que deberán tenerse en cuenta para el control de los accesos a las redes, a los sistemas operativos y a las aplicaciones corporativas. Así mismo, deberán considerarse qué privilegios son los adecuados para cada usuario o cuáles son las responsabilidades que el usuario tiene para la protección de su puesto de trabajo.

a) Requisitos de negocio para el control de accesos

1. Política de control de accesos.
2. Control de acceso a las redes y servicios asociados.

b) Gestión de acceso de usuario

1. Gestión de altas y bajas en el registro de usuarios.
2. Gestión de los derechos de acceso asignados a los usuarios.
3. Gestión de los derechos de acceso con privilegios especiales.
4. Gestión de información confidencial de autenticación de usuarios.
5. Revisión de los derechos de acceso de los usuarios.
6. Retirada o adaptación de los derechos de acceso.

c) Responsabilidades del usuario

1. Uso de información confidencial para la autenticación.

d) Control de acceso al sistema y aplicaciones

1. Restricción del acceso a la información.
2. Procedimientos seguros de inicio de sesión.
3. Gestión de contraseñas de usuario.
4. Uso de herramientas de administración de sistemas.
5. Control de acceso al código fuente de los programas.

- **Cifrado.** Se contempla el cifrado de la información con el fin de delimitar su acceso y garantizar su integridad.
    1. Política de uso de los controles criptográficos.
    2. Gestión de claves.
- **Seguridad física y ambiental**. Las medidas de seguridad física y del entorno quedan recogidas en dos controles de este apartado. Por una parte, se establecen los requerimientos físicos de los edificios, como el establecimiento de

perímetros de seguridad, zonas de carga o controles físicos de entrada y, por otra, la seguridad de los equipos, considerando el suministro o el mantenimiento de los mismos.

a) **Áreas seguras.**

1. Perímetro de seguridad física.
2. Controles físicos de entrada.
3. Seguridad de oficinas, despachos e instalaciones.
4. Protección contra las amenazas externas y ambientales.
5. El trabajo en áreas seguras.
6. Áreas de acceso público, carga y descarga.

b) **Seguridad de los equipos.**

1. Emplazamiento y protección de equipos.
2. Instalaciones de suministro.
3. Seguridad del cableado.
4. Mantenimiento de los equipos.
5. Salida de activos fuera de las dependencias de la empresa.
6. Seguridad de los equipos y activos fuera de las instalaciones.
7. Reutilización o retirada segura de dispositivos de almacenamiento.
8. Equipo informático de usuario desatendido.
9. Política de puesto de trabajo despejado y bloqueo de pantalla.

- **Seguridad en las operaciones**. La operación de las comunicaciones debería estar procedimentada adecuadamente, estableciendo de manera clara las responsabilidades que, en materia de operación, deban considerarse. En este apartado se incluye también la supervisión de los servicios que son contratados a terceros y la planificación de los requisitos y necesidades de seguridad de los sistemas.

a) Responsabilidades y procedimientos de operación.

1. Documentación de procedimientos de operación.
2. Gestión de cambios.
3. Separación de entornos de desarrollo, prueba y producción.

b) Protección y controles contra código malicioso.

c) Copias de seguridad de la información.

d) Registro de actividad y supervisión.

1. Registro y gestión de eventos de actividad.
2. Protección de los registros de información.
3. Registros de actividad del administrador y operador del sistema.
4. Sincronización de relojes.

e) Control del software en explotación.

1. Instalación del software en sistemas en producción.

f) Gestión de la vulnerabilidad técnica.

1. Gestión de vulnerabilidades técnicas
2. Restricciones en la instalación de software.

g) Controles de auditoría de los sistemas de información.

- **Seguridad en las telecomunicaciones.** Deben controlarse las comunicaciones del sistema mediante la implantación de ciertos mecanismos de intercambio de información.

a) Gestión de la seguridad en las redes.

1. Controles de red.
2. Mecanismos de seguridad asociados a servicios en red.
3. Segregación de redes.

b) Intercambio de información con partes externas.

1. Políticas y procedimientos de intercambio de información.

2. Acuerdos de intercambio.
3. Mensajería electrónica.
4. Acuerdos de confidencialidad y secreto.

- **Adquisición, desarrollo y mantenimiento de sistemas**. Este sistema propone que los sistemas debieran contar con unos requisitos de seguridad específicos que abarcan desde la entrada de los datos hasta el control del software y las medidas de seguridad de los procesos de desarrollo de software. En este apartado se considera además el control de las vulnerabilidades técnicas.

a) Requisitos de seguridad de los sistemas de información.

1. Análisis y especificación de los requisitos de seguridad.
2. Seguridad de las comunicaciones en servicios accesibles por redes públicas.
3. Protección de las transacciones por redes telemáticas.

b) Seguridad en los procesos de desarrollo y soporte.

1. Política de desarrollo seguro de software.
2. Procedimientos de control de cambios en los sistemas.
3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
4. Restricciones a los cambios en los paquetes de software.
5. Uso de principios de ingeniería en protección de sistemas.
6. Seguridad en entornos de desarrollo.
7. Externalización del desarrollo de software.
8. Pruebas de funcionalidad durante el desarrollo de los sistemas.
9. Pruebas de aceptación.

c) Protección de los datos utilizados en pruebas.

- **Relaciones con suministradores.** En este apartado se aborda la seguridad de la información con suministradores y contratistas.

a) **Seguridad de la información en las relaciones con suministradores.**
   1. Política de seguridad de la información para suministradores.
   2. Tratamiento del riesgo dentro de acuerdos de suministradores.
   3. Cadena de suministro en tecnologías de la información y comunicaciones.

b) **Gestión de la prestación del servicio por suministradores.**
   1. Gestión de la prestación del servicio por suministradores.
   2. Supervisión y revisión de los servicios prestados por terceros.

- **Gestión de incidentes**. Deberá establecerse cuáles son los canales de comunicación de eventos y debilidades y cómo será el proceso de gestión de incidencias.
   1. Responsabilidades y procedimientos.
   2. Notificación de los eventos de seguridad de la información.
   3. Notificación de puntos débiles de la seguridad.
   4. Valoración de eventos de seguridad de la información y toma de decisiones.
   5. Respuesta a los incidentes de seguridad.
   6. Aprendizaje de los incidentes de seguridad de la información.
   7. Recopilación de evidencias.

- **Gestión de continuidad del negocio**. Este apartado establece los requisitos que deberían considerarse en relación a garantizar la continuidad de los servicios críticos del negocio. Cumplimiento legal. Podemos considerar este apartado como garantía del cumplimiento de las exigencias legales que cada organización tiene. Además, se incluyen en este apartado las consideraciones que deben tenerse en cuenta en la auditoría de los sistemas.

a) **Continuidad de la seguridad de la información.**
   1. Planificación de la continuidad de la seguridad de la información.

2. Implantación de la continuidad de la seguridad de la información.
3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

b) Redundancias.

1. Disponibilidad de instalaciones para el procesamiento de la información.

- **Cumplimiento.** Este último punto es de vital importancia, ya que supone la adecuación a la legislación vigente así como el cumplimiento de las obligaciones contractuales, y además se incluyen las revisiones del proceso tanto para su depuración como para asegurar el cumplimiento del mismo.

a) Cumplimiento de los requisitos legales y contractuales.

1. Identificación de la legislación aplicable.
2. Derechos de propiedad intelectual.
3. Protección de los registros de la organización.
4. Protección de datos y privacidad de la información personal.
5. Regulación de los controles criptográficos.

b) Revisiones de la seguridad de la información.

1. Revisión independiente de la seguridad de la información.
2. Cumplimiento de las políticas y normas de seguridad.
3. Comprobación del cumplimiento.

5.3.4 Checklist

Para llevar a cabo un proceso adecuado de control y auditoria, se ha creado la siguiente checklist para facilitar el trabajo del auditor.

Tabla 2. Checklist ISO 27002

Nº	Objeto de Control	Control	Aplica (%)
1	Política de Seguridad de la información.	OBJETIVO: La Dirección debe proporcionar indicaciones y apoyar la seguridad de la información de acuerdo con los requisitos del negocio y con la legislación y las normativas aplicables.	
1.1	Documento de política de seguridad de la información.	Existe un documento publicado de la Dirección de la empresa que recoge la política de seguridad de la información que se distribuye a los empleados y a posibles terceros implicados.	
1.2	Revisión de la política de seguridad de la información.	La política de seguridad de la información se revisa de forma periódica de forma planificada y cuando se producen cambios significativos para asegurar su corrección y eficacia.	
2	Aspectos organizativos.	OBJETIVO: Gestión de la seguridad de la información dentro de la organización.	
2.1	Compromiso de la Dirección con la seguridad de la información.	La Dirección presta un apoyo activo a la seguridad de la información dentro de la organización mediante directrices claras e inequívocas, un compromiso patente, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información.	
2.2	Coordinación de la seguridad de la información.	Las actividades relativas a la seguridad de la información se coordinan entre los representantes de las diferentes áreas de la organización atendiendo a sus correspondientes roles y funciones.	
2.3	Asignación de responsabilidades relativas a la seguridad de la información.	Están claramente definidas todas las responsabilidades relativas a la seguridad de la información.	
2.4	Segregación de tareas	Las tareas y áreas de responsabilidad están bien diferenciadas para reducir la posibilidad de que se produzcan modificaciones no autorizadas y usos indebidos de los activos de la organización	
2.5	Proceso de autorización de recursos para el tratamiento de la información.	La Dirección ha definido procesos de autorización para los nuevos recursos del tratamiento de la información	
2.6	Contactos con las autoridades.	Se mantienen los contactos adecuados con las autoridades competentes.	
2.7	Contactos don grupos de especial interés	Se mantienen los contactos adecuados con grupos de interés especial tales como asociaciones profesionales y/o especialistas en seguridad de la información.	
2.8	Dispositivos para movilidad y teletrabajo.	Existe una política de seguridad específica para el empleo de dispositivos móviles y de teletrabajo.	

Nº	Objeto de Control	Control	Aplica (%)
3	Recursos humanos.	OBJETIVO: Establecer las medidas de seguridad que deben considerarse en cada una de las fases de desempeño de trabajo.	
3.1	Funciones y responsabilidades.	Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros están definidas conforme a la política de seguridad de la información de la organización.	
3.2	Investigación de antecedentes.	Se realizan comprobaciones de los antecedentes de todos los candidatos al puesto de trabajo, de los contratistas o de los terceros, conforme a la legislación vigente y de forma proporcionada a los requisitos del puesto, la criticidad de la información que se maneja y a los riesgos posibles.	
3.3	Términos y condiciones de contratación.	Los empleados, los contratistas y los terceros aceptan y firman los términos y condiciones de su contrato de trabajo. Dichos términos establecen sus responsabilidades y las de la organización en lo relativo a seguridad de la información.	
3.4	Responsabilidades de gestión.	La Dirección exige a los empleados y terceros implicados que apliquen la seguridad acorde a lo establecido en las políticas y procedimientos de la organización.	
3.5	Concienciación, educación y capacitación en Seguridad de la Información.	Los empleados reciben formación adecuada de forma periódica acorde al desempeño propio del puesto de trabajo.	
3.6	Proceso disciplinario.	Existe un proceso disciplinario para los empleados que incumplan la política de seguridad de la información.	
3.7	Cese o cambio del puesto de trabajo.	Existe una política para la devolución de activos. Los derechos de acceso se retiran, en caso de cese, o cambian acorde al nuevo puesto de trabajo del empleado o contratista.	
4	Gestión de Activos	OBJETIVO: Alcanzar una protección adecuada para los activos de la organización.	
4.1	Inventario de activos.	Todos los activos están identificados. Existe un inventario de activos que los incluye a todos.	
4.2	Propiedad de los activos.	Todos los activos relacionados con el tratamiento de la información tienen un propietario o responsable.	
4.3	Empleo de los activos.	Existen reglas relativas al uso adecuado de los activos y de la información dentro de la organización.	
4.4	Devolución de los activos.	Existe un proceso reglado de devolución de los activos en caso de deterioro o cese de la actividad.	
4.5	Clasificación de la información.	Existe normativa acerca de quién, cómo y en qué circunstancias puede manipular los activos relacionados con la seguridad de la información.	
4.6	Manipulación de activos.	Existe normativa acerca de quién, cómo y en que circunstancias puede manipular los activos relacionados con la seguridad de la información.	
4.7	Soportes de almacenamiento.	Existen restricciones al uso de soportes extraíbles, así como un protocolo de destrucción de soportes y de tratamiento de soportes en tránsito.	

Nº	Objeto de Control	Control	Aplica (%)
5	Control de accesos	OBJETIVO: Prevenir accesos no autorizados al sistema o a la información de la organización.	
5.1	Política de control de accesos	Existe una política para reglar el control del acceso de los usuarios a la información y al sistema.	
5.2	Control de acceso a las redes y servicios asociados.	El acceso a las redes se controla mediante el uso de cuentas de usuario o similar. Se guarda registro de tales accesos.	
5.3	Gestión de altas y bajas en el registro de usuarios.	Existe un mecanismo reglado de altas y bajas de los usuarios. Existe un documento de solicitud de alta validado por el responsable último de la misma. Existe un documento de notificación de baja en el que se exponen los motivos de la misma.	
5.4	Gestión de los derechos de acceso asignados a los usuarios.	Existe un procedimiento distintos perfiles de usuario con diferentes niveles o derechos de acceso atendiendo al desempeño del puesto.	
5.5	Gestión de los derechos de acceso con privilegios especiales.	Existen perfiles con derechos de acceso especiales. Existe un procedimiento para la gestión de este tipo de usuarios restringido y controlado.	
5.6	Gestión de información confidencial de autenticación de usuarios.	Existe una correcta gestión de la información confidencial de autenticación de los usuarios (claves). Las claves se almacenan cifradas. Las claves se cifran en su procesamiento. Se exige a los usuarios el empleo de buenas prácticas de seguridad en el uso de información confidencial. ¿Existen inventarios u hojas de passwords? ¿Se encuentran debidamente protegidas?	
5.7	Revisión de los derechos de acceso de los usuarios.	Los derechos de acceso se revisan frecuentemente.	
5.8	Retirada y adaptación de los derechos de acceso de los usuarios.	Los derechos de acceso se adaptan ante cambios de puesto/desempeño por parte del usuario. Se retiran los derechos de acceso por incumplimientos de seguridad o cese de actividad.	
5.9	Restricción de acceso a la información.	Los usuarios tienen restringido el acceso acorde a una política de control de accesos definida.	
5.10	Control de acceso a sistema y aplicaciones.	Se controla el acceso mediante políticas de log-on seguras.	
5.11	Gestión de contraseñas de usuario.	Los empleados están informados sobre la idoneidad del uso de contraseñas adecuadas. Existen sistemas de gestión de contraseñas que aseguran la calidad de las mismas.	
5.12	Uso de herramientas de administración de sistemas.	Está prohibido el empleo de software que anule o evite controles en las aplicaciones y sistemas.	
5.13	Control de acceso al código fuente.	El acceso al código fuente se encuentra controlado y restringido.	

Nº	Objeto de Control	Control	Aplica (%)
6	Cifrado	OBJETIVO: Se persigue el uso de técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad	
6.1	Política de uso de los controles criptográficos	Existe una política definida para el empleo de controles criptográficos.	
6.2	Gestión de claves de cifrado	Existe una política sobre la creación, uso y ciclo de vida de las claves de cifrado.	
7	Seguridad física y ambiental	OBJETIVO: Prevenir accesos físicos no deseados así como daños a las instalaciones. Evitar pérdidas, daños y robos en los activos de la organización.	
7.1	Perímetro de seguridad.	Existe un perímetro de seguridad (barreras, puestos de control).	
7.2	Controles físicos de entrada.	Existen controles físicos de acceso a las zonas desde las que se puede acceder a la información.	
7.3	Seguridad de oficinas, despachos y recursos.	Existen medidas de seguridad física para las instalaciones.	
7.4	Amenazas ambientales.	Existen medidas para prevenir daños por fuego, agua o terremotos, entre otros.	
7.5	Trabajo en áreas seguras	Existen directrices para el trabajo en áreas seguras, son públicas y accesibles para los empleados afectados.	
7.6	Áreas de acceso público, carga y descarga.	Existen controles sobre los puntos de acceso púbico tales como áreas de carga y descarga. Dichos puntos se encuentran aislados de las zonas donde se produce el tratamiento de la información	
7.7	Emplazamiento y protección de equipos.	Los equipos se encuentran protegidos de las amenazas ambientales así como de los accesos no autorizados.	
7.8	Instalaciones de suministro.	Los equipos se encuentran protegidos contar cortes de suministro.	
7.9	Seguridad del cableado.	El cableado está protegido frente a daños y sabotajes.	
7.10	Mantenimiento de los equipos.	Los equipos reciben de forma periódica mantenimiento para su correcta usabilidad.	
7.11	Seguridad de equipos y activos fuera de las instalaciones.	Se aplica un protocolo de seguridad para los equipos o activos que salen de las instalaciones, ya sea por transporte u otros fines, tales como teletrabajo.	
7.12	Reutilización y retirada de dispositivos de almacenamiento.	Los soportes se comprueban y se borran debidamente antes de su retirada.	
7.13	Equipo de usuario desatendido.	Los equipos informáticos desatendidos están correctamente protegidos frente a accesos no autorizados.	
7.14	Política de puesto despejado y bloqueo de pantalla.	Existen políticas de bloqueo de pantalla/sesión automáticas. Se informa a los usuarios de que no deben tener claves o datos sensibles en sus puestos de trabajo.	

Nº	Objeto de Control	Control	Aplica (%)
8	Seguridad en las operaciones	OBJETIVO: Asegurar el funcionamiento correcto y seguro de los recursos de tratamiento de la información.	
8.1	Documentación de procedimientos de operación.	Los procesos de operaciones están debidamente documentados y son accesibles para todos aquellos que los necesitan.	
8.2	Gestión de cambios.	Se controlan los cambios en los recursos y en los sistemas.	
8.3	Separación de entornos de desarrollo, prueba y producción.	Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado a los datos o cambios en el sistema en producción.	
8.4	Protección contra código malicioso.	Existen controles para prevenir el código malicioso, así como herramientas para la recuperación del sistema. Los usuarios están formados y concienciados sobre el mismo.	
8.5	Copias de seguridad de la información.	Se efectúan de forma periódica copias de seguridad de la información y del resto del software. Dichas copias se prueban periódicamente para confirmar su corrección y utilidad.	
8.6	Registro de actividad y supervisión.	Se registran las actividades de operación y administración sobre el sistema.	
8.7	Protección de los registros de información.	Los dispositivos y la información se encuentran debidamente protegidos contra accesos y modificaciones indebidas.	
8.8	Sincronización de relojes.	Los dispositivos de la organización están sincronizados a efectos de registro de actividades e información.	
8.9	Registro de eventos de actividad.	Se generan registros de auditoría de las acciones de los usuarios, de las excepciones del sistema y de los eventos de seguridad (accesos, etc.).	
8.10	Control del software en explotación.	Se controla la instalación del software en los equipos. No se permite instalar software no autorizado o validado.	
8.11	Gestión de vulnerabilidades técnicas.	Se hacen frecuentes revisiones del software base y se instalan los parches necesarios en caso de haberlos. Las instalaciones de parches se realizan con rapidez (poca latencia). Existen protocolos de actualización/parcheo de software.	

Nº	Objeto de Control	Control	Aplica (%)
9	Seguridad en las telecomunicaciones.	OBJETIVO: Asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.	
9.1	Controles de red.	Existen medidas de control de red tales como proxies y cortafuegos. Se recopilan y estudian las estadísticas de estas herramientas tales como ataques detectados, accesos prohibidos a internet u otros recursos de la intranet…	
9.2	Segregación de redes	Existen redes separadas para los distintos grupos de la organización y los usuarios.	
9.3	Políticas de intercambio de información.	Existen procedimientos y controles para el intercambio de información con entidades externas. Existen acuerdos de interfaz con las entidades externas que incluyen la transferencia segura de información.	
9.4	Mensajería electrónica.	Existen controles sobre la información que se entrega a terceros (clientes). Se eliminan los metadatos en la información enviada a terceros.	
9.5	Acuerdos de confidencialidad.	Se revisa periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información, y se definen dichos acuerdos en caso de ser necesario.	
10	Adquisición, desarrollo y mantenimiento de sistemas.	OBJETIVO: Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.	
10.1	Política desarrollo de software.	Existe una política de desarrollo de software clara y pública para los desarrolladores (empleados o contratistas), de obligado cumplimiento. Esta política se revisa periódicamente.	
10.2	Control de cambios.	Existen procedimientos específicos para el control de los cambios en los sistemas de la información.	
10.3	Revisión técnica de las aplicaciones tras cambios.	Se realizan comprobaciones (sanity checks) de las plataformas después de realizar cambios para comprobar la integridad y la disponibilidad de la plataforma mediante procedimientos regulados.	
10.4	Restricciones a los cambios en los paquetes de software.	No se permiten las modificaciones sobre software proporcionado por terceros.	
10.5	Seguridad en entornos de desarrollo.	Los entornos no productivos están debidamente securizados y su acceso controlado. Los datos para las pruebas de los entornos de desarrollo no son datos reales.	
10.6	Externalización del desarrollo de software.	Se mantienen controles y supervisión sobre las actividades de desarrollo subcontratadas.	
10.7	Pruebas de funcionalidad durante el desarrollo.	Se realizan pruebas de funcionalidad en los entornos no productivos referidas a la seguridad.	
10.8	Pruebas de aceptación.	La aceptación de nuevos SI, así como de actualizaciones sobre los mismos, está reglada y sujeta a pruebas.	

Nº	Objeto de Control	Control	Aplica (%)
11	Gestión de la prestación del servicio por suministradores.	OBJETIVO: Mantener el nivel en la prestación de servicios conforme a los acuerdos establecidos con el proveedor.	
11.1	Política de seguridad de la información para suministradores.	Los requisitos de seguridad de la información requeridos a los suministradores se encuentran recogidos documentalmente.	
11.2	Cadena de suministro en tecnologías de la información y comunicaciones	Existe una evaluación de riesgos relativa al manejo de sistemas e información por parte de terceros. Existen contratos de confidencialidad y uso correcto de los sistemas para los suministradores. Se exige algún tipo de certificación a los proveedores relativa a la seguridad de la información (ISO 27001).	
11.3	Supervisión y revisión de los servicios prestados por terceros.	Existen unos niveles de servicio (SLA) establecidos y concretos cuyo cumplimiento se controla regularmente. Existen sanciones para los proveedores en caso de incumplimiento.	
12	Gestión de incidentes.	OBJETIVO: Garantizar que se aplican las acciones correctivas a tiempo para los eventos de seguridad y las debilidades relativas a los sistemas de información.	
12.1	Responsabilidades y procedimientos.	Las responsabilidades relativas a las posibles incidencias de seguridad de la información están claramente definidas.	
12.2	Notificación de los eventos de seguridad de la información y debilidades.	Existen canales para la rápida notificación de incidentes en la seguridad de la información o ante la detección de posibles debilidades en el sistema. Todos los empleados y suministradores los conocen y utilizan de forma obligatoria.	
12.3	Valoración de eventos de seguridad de la información.	Los eventos de seguridad se recogen y evalúan, y se clasifican como incidentes en caso de ser necesario para su estudio y corrección.	
12.4	Respuesta a los incidentes de seguridad y aprendizaje de los mismos.	Existe un procedimiento para el estudio de los casos post-incidente (post-mortem) que permita determinar el problema y su posible solución, así como las responsabilidades devengadas.	
12.5	Recopilación de evidencias.	Existe un estándar relativo a la información que debe ser recogida y preservada ante incidentes en la seguridad de la información para su futuro análisis.	
13	Gestión de la continuidad del negocio.	OBJETIVO: Mantener la seguridad de la información en los sistemas de gestión de continuidad de negocio.	
13.1	Continuidad de la seguridad de la información.	Existen procedimientos de actuación en caso de desastre o crisis. Se revisan periódicamente para comprobar su eficacia, realizando pruebas de validez regularmente o ante cambios significativos en los sistemas. Están definidos los requisitos de seguridad de la información ante situaciones de crisis o desastre.	
13.2	Redundancia.	Existen componentes y/o arquitecturas redundantes para garantizar la continuidad del negocio. Se realizan pruebas regulares que garanticen la correcta conmutación a los sistemas redundantes.	

		Se realizan mediciones en caso de error (*failover*) para la mejora de las actuaciones.	

Nº	Objeto de Control	Control	Aplica (%)
14	Cumplimiento.	Evitar incumplimientos a relativos a la seguridad de la información, especialmente legales y contractuales.	
14.1	Cumplimiento de los requisitos legales y por contrato.	Se dispone de asesoramiento legal interno o externo. Existe documentación relativa a los requisitos que deben cumplir los sistemas en lo referente a la legislación, normativa y contratos aplicables.	
14.2	Derechos de propiedad intelectual.	Existen procedimientos para garantizar el Derecho a la Propiedad Intelectual. El software empleado es original.	
14.3	Protección de los registros de la organización.	Los registros se encuentran protegidos frene a accesos, manipulaciones o publicaciones no autorizadas, así como ante la destrucción de los mismos.	
14.4	Protección de datos de carácter personal.	Se garantiza la protección de los datos de carácter personal.	
14.5	Regulación de los controles criptográficos	Existen controles de cifrado de la información conforme a la legislación vigente.	
14.6	Revisión independiente de la seguridad de la información.	Se realizan Auditorías externas de la seguridad de la información de forma regular.	
14.7	Cumplimiento de las políticas y normas de seguridad.	Se realizan controles regulares dentro de las áreas de responsabilidad. Se realizan auditorías internas regularmente (ISO 19011).	

Tal y como puede observarse, mediante la aplicación de la norma ISO 27001/27002 disponemos de una herramienta eficaz y detallada, concisa y actualizada (2013) que permite asegurar unos niveles correctos en lo que a seguridad de la información se refiere dentro de cualquier organización.

CAPÍTULO 6

CONCLUSIONES Y FUTURAS LÍNEAS DE TRABAJO

En cuanto a las líneas futuras de actuación, vamos a diferenciar las de los usuarios particulares y las de los proveedores de los servicios de las RRSSO.

En primer lugar, los particulares deben ser conscientes de que su información e imagen son valiosas, y de que existen riesgos tanto en las RRSSO como en el uso de Internet.

En este sentido, hay que ser consciente de qué tipo de información se aporta a las RRSSO y tener claro su fin, así como asegurarnos de no otorgar información excesiva y ser conscientes de los riesgos ya reseñados, adoptando prácticas de buen uso para minimizar el impacto de los mismos.

Se debe prestar una atención especial a los menores ya que son un colectivo con más riesgo y mayor indefensión, inculcándoles un uso correcto y responsable de las RRSSO y otorgándoles conocimiento sobre sus derechos como usuarios, adoptando las medidas indicadas en capítulos previos tales como acompañarles en la navegación o la instalación de herramientas de control parental,

En cuanto a los proveedores de servicios, hay varias líneas que deben mejorar en mi modesta opinión.

Deben mejorarse los contratos de usuario final de modo que sean más comprensibles por parte de los usuarios, dado que el elaborado lenguaje con el que se suelen escribir invita a los usuarios a no leerlos, o incluso, a no entender debidamente el contenido de los mismos aun habiéndolos leído.

Así mismo, deben mejorarse los controles de acceso a las plataformas para asegurar la no existencia de perfiles falsos de usuario, así como la edad de los usuarios que pueden acceder a la plataforma, algo que se está realizando de modo incipiente con analizadores de lenguaje e incluso con mecanismos de control biométrico, aunque su difusión es relativamente escasa.

También se debe mejorar en la información al usuario acerca de sus derechos y de los riesgos de las plataformas, para un mejor uso de las mismas.

Debe facilitarse la denuncia para aquellos casos en los que los usuarios sean víctimas de algún tipo de delito o abuso.

Evitar la publicidad excesiva y lesiva a los usuarios mediante controles a los anunciantes de las plataformas.

Continuar en la mejora de la seguridad de la información de los usuarios otorgando herramientas a los mismos para que la difusión de su información sea limitada, o al menos, tan extensa como el usuario desee, pero no más.

En este sentido, deben adoptarse medidas tales como perfiles restringidos en el momento de la creación del mismo, etiquetado de contenidos, posibilidad de denunciar contenidos lesivos de forma ágil…

Por último, se aconseja la adopción de medidas de control y seguridad tales como las normas ISO27001/27002 antes expuestas para evitar casos de sabotaje, robo de información y otro tipo de incidentes que puedan causar una vulneración de los derechos de los usuarios, de la legalidad vigente o de los intereses de la propia entidad.

A modo de conclusión, diremos que las redes sociales online han supuesto una revolución en la comunicación global, y que debido a sus características es previsible que lo hagan durante mucho tiempo.

Si aceptamos como cierta esta afirmación, es necesario estar debidamente concienciados y preparados para hacer uso de ellas de modo seguro, del mismo modo que los proveedores de servicios deben entender que cada vez nos volveremos usuarios más formados, y más conscientes de nuestros derechos, lo que nos hará más exigentes en cuanto a la usabilidad, pero también en lo tocante a la seguridad.

Si repasamos los objetivos planteados al comienzo de la exposición parece, en mi modesta opinión, que se han cumplido.

Comenzaremos por revisar los objetivos intermedios.

En primer lugar se ha explicado que son las RRSSO y la causa de su espectacular crecimiento, así como su origen e incluso algunas clasificaciones frecuentes.

Así mismo, se han puesto en conocimiento del usuario de las RRSSO sus derechos. A este respecto, quiero indicar que se han incluido las normas y leyes en el texto principal (excepto la LOPD que ha sido analizada en detalle) y no en los anexos por varios motivos. En primer lugar porque entiendo que son demasiadas para penalizar en exceso la lectura, y en segundo lugar porque quiero realzar la importancia de las mismas: los usuarios tenemos derechos, existen leyes que los sustentan y sanciones para los infractores.

Igualmente considero cumplido el último objetivo intermedio, dado que se han identificado un gran número de riesgos y amenazas dentro de las RRSSO

Si repasamos ahora los objetivos principales, a saber, elaborar una serie de recomendaciones para los usuarios y sugerir un estándar a los profesionales que supusiese una forma eficaz de evitar los riesgos comentados entiendo que también han sido abordados ambos (en el capítulo 5).

Por último, me gustaría indicar que, en lo personal, el desarrollo de este proyecto me ha ayudado a comprender mejor la realidad de las redes sociales, sobre las que pensaba que conocía mucho al comienzo del PFC, resultando que desconocía aún más.

También quiero indicar que el estudio sobre la ISO27001 me ha facilitado una nueva herramienta de trabajo, así como nuevas oportunidades profesionales.

CAPÍTULO 7

PLANIFICACIÓN Y PRESUPUESTO

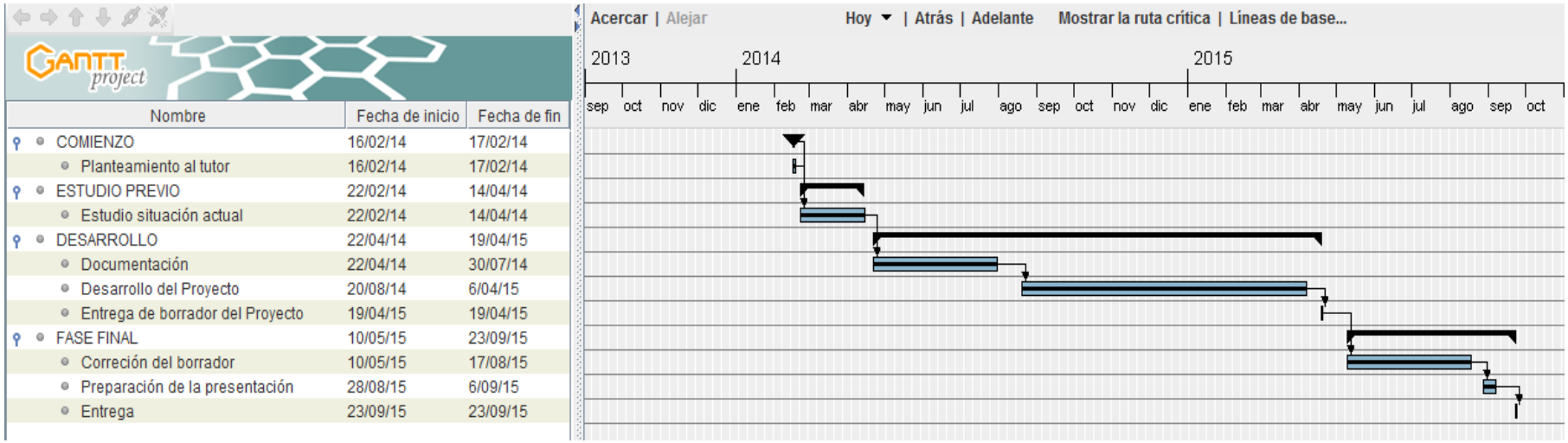
7.1 Introducción

Se recoge en este capítulo la planificación del proyecto y los costes incurridos para la elaboración del mismo.

7.2 Diagrama Gantt del proyecto.

En el siguiente diagrama Gantt se detalla el desarrollo de las distintas fases del proyecto:

Fig. 17. Gantt planificación.



Pasaremos a describirlas más detalladamente debido a la escala del gráfico.

El **planteamiento** al tutor se produjo el 16/02/2014 y tras un intercambio de impresiones sobre el planteamiento inicial, comenzó el **estudio de la situación actual** de las Redes Sociales Online y su problemática, tarea que finalizó el día 14/04/2014.

A la semana siguiente (22/04/2014) se empezó la **documentación** del proyecto, esto es, se profundizó en la problemática encontrada, y se estudiaron tanto la legislación actual (nacional e internacional), noticias surgidas, así como las posibles alternativas para la solución propuesta.

Un mes después, debido a las vacaciones estivales, se comenzó la tarea de desarrollo, en la que se desglosó la información, se unificó y se expuso ordenadamente, plasmando las alternativas elegidas y elaborando las conclusiones.

En la fase final, se revisaron los enlaces web empleados como referencias, se revisó la integridad de la memoria, así como la exposición y ortografía del documento.

Se han tenido en total 496 jornadas (ya excluidos los retardos entre fases), a razón de una hora de trabajo al día.

7.3 Presupuesto.

En este apartado se describen los costes incurridos para la elaboración del proyecto empleando una plantilla estándar de la UC3M facilitada por el tutor.

Fig. 18. Presupuesto.

UNIVERSIDAD CARLOS III DE MADRID

Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor: Anatolio Garrosa Fernandes

2.- Departamento: Informática

3.- Descripción del Proyecto:

- Titulo: **Redes Sociales. Uso responsable y controles.**
- Duración (meses): **16,5**

Tasa de costes Indirectos: 20%

4.- Presupuesto total del Proyecto (valores en Euros):

Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a titulo informativo)	Categoría	Dedicación (hombres mes) [a]	Coste hombre mes	Coste (Euro)	Firma de conformidad
		Ingeniero			0,00	
		Ingeniero Senior		4.289,54	0,00	
Garrosa Fernandes, Anatolio		Ingeniero	3,8	2.694,39	10.238,68	
					0,00	
					0,00	
		Hombres mes 3,8		**Total**	10.238,68	

[a] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d]
PC Portátil	278,00	100	4	60	17,61
		100		60	0,00
		100		60	0,00
		100		60	0,00
		100		60	0,00
					0,00
				Total	17,61

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} \text{xCxD}$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación (60 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
	Total	0,00

OTROS COSTES DIRECTOS DEL PROYECTO[e]

Descripción	Empresa	Costes imputable
	Total	0,00

[e] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas,

6.- Resumen de costes

Presupuesto Costes Totales	Presupuesto Costes Totales
Personal	10.239
Amortización	18
Subcontratación de tareas	0
Costes de funcionamiento	0
Costes Indirectos	2.051
Total	12.308

Como se observa, tan sólo se han incurrido en los costes derivados del salario de la persona que lo ha realizado y un ordenador portátil con el que se ha efectuado el trabajo.

Dos notas al respecto: el software empleado no debe imputarse debido a que el equipo adquirido para la realización del proyecto ya lo traía instalado, y algo similar ocurre con el acceso a internet, que no debe imputarse ya que se ha hecho uso de la conexión de la escuela politécnica.

CAPÍTULO 8

GLOSARIO

AEAT:	Agencia Estatal de Administración Tributaria
AEPD:	Agencia Española de Protección de Datos
AN:	Audiencia Nacional
BIT:	Brigada de Investigación Tecnológica
BOE:	Boletín Oficial del Estado
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart (Prueba de Turing Automática para diferenciar Humanos y Computadoras)
CE:	Constitución Española
CNN:	Cable News Network, cadena de noticias estadounidense
DNS:	Domain Name System (Sistema de Nombres de Dominio)
DoS:	Denial of Service (Denegación de Servicio)
EULA:	End User License Agreement (Acuerdo de usuario final)
INCIBE:	Instituto Nacional de Ciberseguridad de España (antes INTECO)
INTECO:	Instituto Nacional de Tecnologías de la Comunicación
IP:	Internet Protocol
LOPD:	Ley Orgánica de Protección de Datos
LORTAD:	Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal
LSSI-CE	Ley de Servicios de la Sociedad de Información y Comercio Electrónico
OBS:	Online Business School
OMPI:	Organización Mundial de la Propiedad Intelectual.
RAI	Registro de Aceptaciones Impagadas
RD:	Real Decreto
RDF	Resource Description Framework (Marco de Descripción de recursos)
RSD:	Red Social Digital

RSO:	Red Social Online
RRSSO:	Redes Sociales Online
SMS:	Short Messaging Service (Servicio de Mensajes Cortos)
SO:	Sistema Operativo
SPARQL:	SPARQL Protocol and RDF Query Language
TIC	Tecnologías de la Información y la Comunicación
TJUE:	Tribunal de Justicia de la Unión Europea
TPV:	Terminal de Punto de Venta
UE:	Unión Europea
XML:	eXtensible Markup Language

CAPÍTULO 9

ANEXOS

Anexo 1

Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea

Antecedentes

Un fallo reciente del Tribunal de Justicia de la Unión Europea (C-131/12, 13 de mayo de 2014) permite que determinados usuarios soliciten que los motores de búsqueda eliminen resultados de consultas que incluyan su nombre si los derechos de privacidad de la persona prevalecen sobre los intereses en esos resultados.

Al realizar esa solicitud, Google realizará una ponderación entre los derechos de privacidad de los usuarios y el derecho del público a conocer y distribuir información. Al evaluar su solicitud, Google examinará si los resultados incluyen información obsoleta sobre usted, así como si existe interés público por esa información (por ejemplo, Google puede negarse a retirar determinada información sobre estafas financieras, negligencia profesional, condenas penales o comportamiento público de funcionarios del gobierno).

Para completar este formulario, necesitará una copia digital de un documento de identificación. Si envía esta solicitud en nombre de otra persona, tendrá que proporcionar un documento de identificación de esa persona. Los campos marcados con un asterisco* se deben completar para poder enviar su solicitud.

Seleccione el país cuya legislación se aplica a su solicitud. *

Seleccionar uno

Información personal

Nombre utilizado para realizar búsquedas *

El nombre completo del que solicita que se retiren los resultados de búsqueda

Nombre completo del solicitante

Su propio nombre, si representa a otra persona (si envía una solicitud en nombre de otra persona, debe tener autorización para actuar en su nombre)

Si envía esta solicitud en nombre de otra persona, debe especificar su relación con ella (por ejemplo, "padre" o "abogado").

Dirección de correo electrónico de contacto *

(dirección a la que se enviarán los correos electrónicos relacionados con su solicitud)

Resultados de búsqueda que quiere que se retiren de la lista de resultados que se produce al buscar el nombre

Para que podamos evaluar su solicitud, necesitamos que haga lo siguiente:
a) Identifique cada resultado de la lista de resultados que quiere que se retire indicando la URL de la página web a la que dirige (la URL se puede encontrar en la barra del navegador después de hacer clic en el resultado de búsqueda en cuestión).
b) Explique los motivos por los que la página web enlazada se refiere a usted (o, si envía este formulario en nombre de otra persona, a esa persona).
c) Explique los motivos por los que la inclusión de cada URL como resultado de búsqueda resulta irrelevante, obsoleto o inaceptable de cualquier otro modo.

URLs de resultados que quiere que se retiren *

Añadir más

Si su solicitud hace referencia a más de un resultado, indique la URL de cada resultado y explique los motivos por los que la inclusión de ese resultado en los resultados de búsqueda resulta irrelevante, obsoleta o inaceptable de cualquier otro modo. Sin esta información, no podremos procesar su reclamación.*

Por ejemplo:

http://ejemplo_1.com

Esta URL hace referencia a mí porque... Esta página no debería incluirse como resultado de búsqueda porque...

http://ejemplo_2.com

Esta URL hace referencia a mí porque... Esta página no debería incluirse como resultado de búsqueda porque...

Para evitar las solicitudes de retirada de contenido fraudulentas de personas que se hacen pasar por otros usuarios, que intentan dañar a sus competidores o que quieren eliminar información legal de forma inadecuada, necesitamos verificar su identidad. **Adjunte una copia legible de un documento que verifique su identidad** (o la identidad de la persona que le ha autorizado para representarla). No es necesario que sea un pasaporte ni otro documento de identificación oficial. Puede ocultar partes del documento (por ejemplo, números), siempre que el resto de la información permita identificarle. Asimismo, puede ocultar la fotografía, excepto si solicita que se retiren páginas que incluyan fotografías suyas. Google solo utilizará esta información para certificar la autenticidad de su solicitud y eliminará la copia en un plazo de un mes después de cerrar su solicitud de retirada de contenido, a menos que la ley establezca lo contrario. *

Declaro que la información de esta solicitud es precisa y que soy la persona afectada por las páginas web identificadas, o que tengo autorización de la persona afectada para enviar esta solicitud. *

Tenga en cuenta que no podemos procesar su solicitud si el formulario no se ha rellenado correctamente o si la solicitud está incompleta.

Firma

Al escribir su nombre y hacer clic en "Enviar", declara que las afirmaciones anteriores son verdaderas, que solicita la retirada de los resultados de búsqueda identificados por las URL que ha indicado anteriormente y que, si actúa en nombre de otra persona, tiene la autoridad legal para hacerlo.

Google Inc. utilizará la información personal que proporcione en este formulario (como su información personal y todos los datos de identificación) para procesar su solicitud y cumplir con nuestras obligaciones legales. Google puede compartir información de su solicitud con las autoridades de protección de datos, pero solo si la solicitan para investigar o revisar una decisión que Google haya tomado. Esto suele ocurrir porque se haya puesto en contacto con la autoridad de protección de datos nacional en relación

con nuestra decisión. Google puede proporcionar información a los webmasters de las URL que se hayan retirado de nuestros resultados de búsqueda.

Firma *

Indique aquí su nombre completo

Firmado el *

MM/DD/AAAA

* Campo obligatorio

Anexo 2

Ejemplo de funcionamiento de un ataque de Inyección SQL.

Asumiendo que el siguiente código reside en una aplicación web y que existe un parámetro "nombreUsuario" que contiene el nombre de usuario a consultar, una inyección SQL para el borrado de datos o la extracción de estos, se podría provocar de la siguiente forma:

El código SQL original es:

consulta := "SELECT * FROM usuarios WHERE nombre = '" + nombreUsuario + "';"

Si el operador escribe un nombre nada anormal sucederá, la aplicación generaría una sentencia SQL perfectamente correcta, en donde se seleccionarían todos los registros con el nombre introducido en la base de datos:

SELECT * FROM usuarios WHERE nombre = 'Pepe';

Pero si un operador malintencionado escribe como nombre de usuario a consultar:

<<Pepe'; DROP TABLE usuarios; SELECT * FROM datos WHERE nombre LIKE '%>>

se generaría la siguiente consulta SQL:

SELECT * FROM usuarios WHERE nombre = 'Pepe';
DROP TABLE usuarios;
SELECT * FROM datos WHERE nombre LIKE '%';

En la base de datos se ejecutaría la consulta en el orden dado, se seleccionarían todos los registros con el nombre 'Pepe', se borraría la tabla 'usuarios' y finalmente se seleccionaría toda la tabla "datos", que no debería estar disponible para los usuarios web comunes.

Hay varias formas de evitar este tipo de ataques:

a) En PHP y para bases de datps MySQL tenemos la función mysql_real_escape_string, que se añade en las variables que se emplean para realizar la consulta:

```
$respuesta=mysql_query("SELECT * FROM `Usuarios` WHERE
`user`='".mysql_real_escape_string($name)."' AND
`pass`='".mysql_real_escape_string($password)."'")
```

b) En .NET evitaremos la inyección en SQL Server (con C#) estableciendo el tipo de parámetro como literal con SqlDbType.VarChar:

```
SqlConnection con = new SqlConnection(_connectionString);
        SqlCommand cmd = new SqlCommand("SELECT * FROM Usuarios WHERE
      user=@user AND pass=@pass", con);
        /* Las variables  son literales, por lo que no podrán hacer la inyección */
        cmd.Parameters.Add("@user", SqlDbType.VarChar, 32).Value = user;
        cmd.Parameters.Add("@pass", SqlDbType.VarChar, 64).Value = password;
```

O también podemos usar la función *AddWithValue*:

```
using( SqlConnection con = (acquire connection) ) {
        con. Open();
        using( SqlCommand cmd = new SqlCommand("SELECT * FROM Usuarios
WHERE user=@user AND pass=@pass", con) ) {
                /* Convertimos también en literales los parámetros */
                cmd.Parameters.AddWithValue("@user", user);
                cmd.Parameters.AddWithValue("@pass", password);
                using( SqlDataReader rdr = cmd.ExecuteReader() ){
                        /* [...] */
                }
        }
}
```

c) En **Java** se puede crear la consulta con los parámetros y posteriormente establecerlos (es decir, reemplazarlos cuando ya son un literal):

```
Connection con = (acquire Connection)
PreparedStatement query = con.prepareStatement("SELECT * FROM Usuarios WHERE user=? AND pass=?");
query.setString(1, user);

query.setString(2, password);
ResultSet rset = query.executeQuery();
```

d) En PERL se puede emplear *placeholder* que al fin y al cabo es igual que con los dos ejemplos anteriores, agregando a la consulta los parámetros (con este método se pone a punto las comillas para evitar las inyecciones *SQL*):

```
$query = $sql->prepare("SELECT * FROM Usuarios WHERE user=? AND pass=?");
$query->execute($user,$password);
```

e) De modo genércio, pueden establecerse CAPTCHAs en los formularios para determinar si la consulta de usuario la está realizando una persona o una máquina.

f) Se deben verificar los datos que introduce el usuario, de modo que, si esperamos un nombre, por ejemplo, tenga un número máximo de caracteres.

g) Asignar privilegios adecuados a los usuarios que realizan las consultas, de modo que no tengan más de los estrictamente necesarios para poder realizarlas.

Además de lo ya indicado, existen herramientas comerciales que permiten evitar las inyecciones SQL, así como auditar el código implementado en busca de vulnerabilidades.

Anexo 3

Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD).
13 de Diciembre de 1999

Artículo 1

Objeto.

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2.

Ámbito de aplicación.

1. *La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.*

   Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

   a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
   b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) *Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.*

2. *El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:*

   a) *A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.*
   b) *A los ficheros sometidos a la normativa sobre protección de materias clasificadas.*
   c) *A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.*

3. *Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:*

   a) *Los ficheros regulados por la legislación de régimen electoral.*
   b) *Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.*
   c) *Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.*
   d) *Los derivados del Registro Civil y del Registro Central de penados y rebeldes.*
   e) *Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.*

Artículo 3.

Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

Artículo 4.

Calidad de los datos.

1. *Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.*
2. *Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.*
3. *Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.*
4. *Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.*

5. *Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*

   No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

   Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. *Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.*
7. *Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.*

Artículo 5.

Derecho de información en la recogida de datos.

1. *Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

   a) *De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
   b) *Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
   c) *De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
   d) *De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. *Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.*
3. *No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.*
4. *Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.*
5. *No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.*

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se

dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6.

Consentimiento del afectado.

1. *El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.*
2. *No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.*
3. *El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.*
4. *En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.*

Artículo 7.

Datos especialmente protegidos.

1. *De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.*

   Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. *Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.*
3. *Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.*
4. *Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.*
5. *Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.*
6. *No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención*

o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8.

Datos relativos a la salud.

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9.

Seguridad de los datos.

1. *El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la*

tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. *No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.*
3. *Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.*

Artículo 10.

Deber de secreto.

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11.

Comunicación de datos.

1. *Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.*
2. *El consentimiento exigido en el apartado anterior no será preciso:*

   a) *Cuando la cesión está autorizada en una ley.*
   b) *Cuando se trate de datos recogidos de fuentes accesibles al público.*

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12.

Acceso a los datos por cuenta de terceros.

1. *No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.*
2. *La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.*

   En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. *Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*
4. *En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.*

Artículo 13.

Impugnación de valoraciones.

1. *Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.*
2. *El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.*
3. *En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.*
4. *La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.*

Artículo 14.

Derecho de consulta al Registro General de Protección de Datos.

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15.

Derecho de acceso.

1. *El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.*
2. *La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.*
3. *El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.*
4.

Artículo 16.

Derecho de rectificación y cancelación.

1. *El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.*
2. *Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.*
3. *La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.*

Cumplido el citado plazo deberá procederse a la supresión.

4. *Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.*
5. *Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.*

Artículo 17.

Procedimiento de oposición, acceso, rectificación o cancelación.

1. *Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.*
2. *No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.*

Artículo 18.

Tutela de los derechos.

1. *Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.*
2. *El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.*

3. *El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.*
4. *Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.*

Artículo 19.

Derecho a indemnización.

1. *Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.*
2. *Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.*
3. *En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.*

Artículo 20.

Creación, modificación o supresión.

1. *La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente*
2. *Las disposiciones de creación o de modificación de ficheros deberán indicar:*

   a) *La finalidad del fichero y los usos previstos para el mismo.*
   b) *Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.*
   c) *El procedimiento de recogida de los datos de carácter personal.*
   d) *La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.*

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. *En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.*

Artículo 21.

Comunicación de datos entre Administraciones públicas.

1. *Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.*
2. *Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.*
3. *No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.*
4. *En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.*

Artículo 22.

Ficheros de las Fuerzas y Cuerpos de Seguridad.

1. *Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.*
2. *La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.*
3. *La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.*
4. *Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.*

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23.

Excepciones a los derechos de acceso, rectificación y cancelación.

1. *Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.*
2. *Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.*
3. *El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.*
4.

Artículo 24.

Otras excepciones a los derechos de los afectados.

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales.

Artículo 25.

Creación.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26.

Notificación e inscripción registral.

1. *Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.*
2. *Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.*
3. *Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.*
4. *El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.*

   En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. *Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.*

Artículo 27.

Comunicación de la cesión de datos.

1. *El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.*
2. *La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.*

Artículo 28.

Datos incluidos en las fuentes de acceso público.

1. *Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.*
2. *Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.*

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. *Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.*

   En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. *Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.*

Artículo 29.

Prestación de servicios de información sobre solvencia patrimonial y crédito.

1. *Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.*
2. *Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los*

interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. *En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.*
4. *Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos.*

Artículo 30.

Tratamientos con fines de publicidad y de prospección comercial.

1. *Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.*
2. *Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.*
3. *En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.*

4. *Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.*

Artículo 31.

Censo promocional.

1. *Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.*
2. *El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.*
3. *Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento.*

   Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. *Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.*

Artículo 32.

Códigos tipo.

1. *Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.*
2. *Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.*

   En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. *Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.*

Artículo 33.

Norma general.

1. *No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización*

previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. *El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.*

Artículo 34.

Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

a) *Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.*
b) *Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.*
c) *Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.*
d) *Cuando se refiera a transferencias dinerarias conforme a su legislación específica.*
e) *Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.*
f) *Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.*

g) *Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.*

h) *Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público.*

Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) *Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.*

j) *Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.*

k) *Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.*

Artículo 35.

Naturaleza y régimen jurídico.

1. *La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.*
2. *En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.*

3. *Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.*
4. *La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:*

   a) *Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.*
   b) *Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.*
   c) *Cualesquiera otros que legalmente puedan serle atribuidos.*

5. *La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.*

Artículo 36.

El Director.

1. *El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.*
2. *Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.*

   En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. *El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.*
4. *El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.*

Artículo 37.

Funciones.

1. *Son funciones de la Agencia de Protección de Datos:*

   a) *Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.*
   b) *Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.*
   c) *Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.*
   d) *Atender las peticiones y reclamaciones formuladas por las personas afectadas.*
   e) *Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.*
   f) *Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la*

adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.

Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta ley orgánica.

Artículo 38.

Consejo Consultivo.

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39.

El Registro General de Protección de Datos.

1. *El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.*
2. *Serán objeto de inscripción en el Registro General de Protección de Datos:*

   a) *Los ficheros de que sean titulares las Administraciones públicas.*
   b) *Los ficheros de titularidad privada.*
   c) *Las autorizaciones a que se refiere la presente Ley.*
   d) *Los códigos tipo a que se refiere el artículo 32 de la presente Ley.*
   e) *Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.*

3. *Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.*

Artículo 40.

Potestad de inspección.

1. *Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.*

   A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. *Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.*

   Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Finalmente, los artículos 41 y 42 hacen referencia a aquellas materias para las que las Comunidades Autónomas tienen transferida la competencia., y en los del título VII de la ley (artículos del 43 al 49) se definen infracciones y las sanciones relativas a las mismas.

Anexo 4

Política de Datos de Facebook.

¿Qué tipo de información recopilamos?

En función de los servicios que utilices, se recopilan diferentes tipos de información relacionada contigo.

Tus acciones y la información que proporcionas.

Recopilamos el contenido y demás información que proporcionas cuando utilizas nuestros servicios, incluido al registrarte para obtener una cuenta, al crear o compartir contenido y cuando envías mensajes o te comunicas con otros usuarios. Esta información puede corresponder a datos incluidos en el contenido que proporcionas o relacionados con él, como el lugar donde se hizo una foto o la fecha de creación de un archivo. También recopilamos información sobre el uso que haces de los servicios; por ejemplo, el tipo de contenido que ves o con el que interactúas, o la frecuencia y la duración de tus actividades.

Las acciones de otros usuarios y la información que proporcionan.

También recopilamos contenido e información que proporcionan otras personas al utilizar nuestros servicios, incluida información sobre ti; por ejemplo, cuando comparten una foto en la que apareces o suben, sincronizan o importan tu información de contacto.

Tus redes y conexiones.

Recopilamos información acerca de las personas y los grupos a los que estás conectado y de qué forma interactúas con ellos; por ejemplo, las personas con las que más te comunicas o los grupos con los que te gusta compartir contenido. También recopilamos información de contacto que proporcionas si subes, sincronizas o importas esta información (por ejemplo, una libreta de direcciones) desde un dispositivo.

Información sobre pagos.

Si utilizas nuestros servicios para realizar compras o transacciones financieras (por ejemplo, al comprar algo en Facebook, realizar una compra en un juego o realizar una donación), recopilamos información sobre la compra o transacción. Esta información incluye tus datos de pago, como tu número de tarjeta de crédito o de débito y otra

información sobre tarjetas, y otros datos sobre cuentas y autenticación, así como información de facturación, envío y contacto.

Información sobre el dispositivo.

Reunimos información acerca de ordenadores, teléfonos u otros dispositivos donde instales o desde los que accedas a nuestros servicios, así como la información generada por dichos dispositivos, dependiendo de los permisos que hayas concedido. Podemos asociar la información que recopilamos de tus diferentes dispositivos; de este modo, nos resulta más sencillo prestar servicios coherentes en todos ellos. Estos son algunos ejemplos de la información de dispositivos que recopilamos:

- Atributos como el sistema operativo, la versión de hardware, la configuración del dispositivo y los nombres y tipos de programas informáticos, la carga de la batería y la intensidad de la señal, así como datos de identificación del dispositivo.
- Ubicaciones del dispositivo, incluida la posición geográfica específica, obtenida a través de señales de GPS, Bluetooth o Wi-Fi.
- Información sobre la conexión, como el nombre del operador de telefonía móvil o del proveedor de servicios de internet, el tipo de navegador, el idioma y la franja horaria, el número de teléfono móvil y la dirección IP.

Información de sitios web y aplicaciones que utilizan nuestros servicios.

Recopilamos información cuando visitas o utilizas sitios web y aplicaciones de terceros que usan nuestros servicios (por ejemplo, cuando ofrecen nuestro botón "Me gusta" o el inicio de sesión con Facebook, o cuando usan nuestros servicios de medición y publicidad). Dicha información incluye datos acerca de los sitios web y las aplicaciones que visitas, tu uso de nuestros servicios en dichos sitios web y aplicaciones, así como datos que el desarrollador o el editor de la aplicación o el sitio web te proporciona a ti o a nosotros.

Información de socios externos.

Recibimos información sobre ti y tus actividades que nos proporcionan socios externos; por ejemplo, información de un socio cuando ofrecemos servicios de forma conjunta o de un anunciante acerca de tus experiencias o interacciones con él.
Empresas de Facebook.
Recibimos información acerca de ti que nos proporcionan empresas pertenecientes a Facebook u operadas por Facebook, de conformidad con sus condiciones y políticas.

¿Cómo utilizamos esta información?

Nos apasiona crear experiencias atractivas y personalizadas para nuestros usuarios. Usamos toda la información de la que disponemos para poder ofrecer y mantener nuestros servicios. El procedimiento es el siguiente:
Proporcionar, mejorar y desarrollar los servicios.
Lo que nos permite ofrecer nuestros servicios, personalizar el contenido y proponerte sugerencias es el uso que hacemos de esta información para comprender cómo usas e interactúas con nuestros servicios y con las personas o las cosas a las que estás conectado y te interesan, tanto dentro como fuera de nuestros servicios.

También usamos la información de la que disponemos para ofrecerte accesos directos y sugerencias. Por ejemplo, podemos sugerir a un amigo tuyo que te etiquete en una foto comparando sus fotos con la información que hemos recogido de tus fotos del perfil o de otras fotos en las que se te ha etiquetado. Si esta opción está habilitada en tu cuenta, puedes controlar si quieres que propongamos a otros usuarios que te etiqueten en fotos a través de la configuración de "Biografía y etiquetado".

Cuando disponemos de información de localización, la utilizamos para adaptar nuestros servicios a tus necesidades y a las de otros usuarios; por ejemplo, te ayudamos a registrar visitas y a encontrar eventos u ofertas en tu zona o a contarles a tus amigos que te encuentras cerca de ellos.

Realizamos encuestas e investigaciones, probamos funciones en fase de desarrollo y analizamos la información de la que disponemos para evaluar y mejorar productos y

servicios, desarrollar nuevos productos o funciones y realizar auditorías y actividades de solución de problemas.

Comunicarnos contigo.
Usamos tu información para enviarte mensajes de marketing, darte a conocer nuestros servicios e informarte acerca de nuestras políticas y condiciones. También usamos tu información para responderte cuando te pones en contacto con nosotros.

Mostrar y medir anuncios y servicios.

Utilizamos la información de la que disponemos para mejorar nuestros sistemas de publicidad y medición, de tal modo que podamos mostrarte anuncios relevantes, tanto en nuestros servicios como en servicios de terceros, y medir la eficacia y el alcance de los anuncios y servicios. Obtén más información sobre cómo anunciarte en nuestros servicios y cómo controlar el modo en el que se usa tu información para personalizar los anuncios que ves.

Fomentar la seguridad y la protección.

La información de la que disponemos nos ayuda a verificar cuentas y actividades, así como a fomentar la seguridad y la protección en nuestros servicios y en servicios de terceros, por ejemplo, investigando actividades sospechosas o infracciones de nuestras condiciones o políticas. Nos esforzamos por proteger tu cuenta; para ello recurrimos a equipos de ingenieros, sistemas automáticos y tecnología avanzada, como el cifrado y el aprendizaje automático. Asimismo, ofrecemos herramientas de seguridad fáciles de usar que añaden un nivel extra de protección a tu cuenta. Para obtener más información sobre cómo fomentar la seguridad en Facebook, accede al servicio de ayuda sobre la seguridad de Facebook.

Utilizamos cookies y tecnologías similares para prestar y mantener nuestros servicios y cada uno de los usos expuestos y descritos en este apartado de nuestra política.
Consulta nuestra política sobre cookies para obtener más información.

¿Cómo se comparte esta información?

Compartir información en nuestros servicios

Los usuarios utilizan nuestros servicios para conectar y compartir contenido entre sí. Para que esto sea posible, compartimos tu información de las siguientes formas:

Personas con las que te comunicas y compartes contenido.

Cuando compartes contenido y te comunicas utilizando nuestros servicios, eliges el público que puede ver lo que compartes. Por ejemplo, si publicas algo en Facebook, seleccionas el público de la publicación, que puede ser un grupo específico de personas, todos tus amigos o miembros de un grupo. Del mismo modo, cuando utilizas Messenger, también eliges las personas a las que quieres enviar fotos o mensajes.

Información pública es cualquier información que compartes con el público en general, la información de tu perfil público o el contenido que compartes en una página de Facebook o en otro foro público. Cualquier usuario puede ver la información pública dentro o fuera de nuestros servicios, y estos datos se pueden consultar o se puede acceder a ellos a través de los motores de búsqueda en internet, las API y los medios tradicionales, como la televisión.

En algunos casos, las personas con las que te comunicas y compartes información pueden descargar o compartir a su vez dicha información con terceras personas dentro y fuera de nuestros servicios. Cuando haces un comentario en la publicación de otra persona o haces clic en "Me gusta" en el contenido que ha publicado en Facebook, esa persona decide qué destinatarios pueden ver tu comentario o tu “Me gusta”.
Si los destinatarios son el público en general, tu comentario también será público.

Personas que ven contenido que otros usuarios comparten acerca de ti.

Otros usuarios pueden utilizar nuestros servicios para compartir información sobre ti con el público que elijan. Por ejemplo, pueden compartir una foto en la que aparezcas,

mencionarte o etiquetarte en un lugar determinado en una publicación o compartir información sobre ti que tú hayas compartido con ellos. Si tienes cualquier duda sobre la publicación de otras personas, la denuncia social es una forma fácil y rápida de pedir ayuda a alguien de confianza.
Aplicaciones, sitios web e integraciones de terceros en nuestros servicios o que utilizan nuestros servicios.

Cuando utilizas aplicaciones, sitios web u otros servicios de terceros que emplean nuestros servicios o están integrados en ellos, estas plataformas pueden recibir información acerca de lo que publiques o compartas. Por ejemplo, si juegas a un juego con tus amigos de Facebook o utilizas el botón "Comentar" o "Compartir" de Facebook en un sitio web, el desarrollador del juego o el sitio web pueden obtener información sobre tus actividades en el juego o recibir un comentario o enlace que compartas desde su sitio web en Facebook. Además, si descargas o utilizas estos servicios de terceros, estos pueden acceder a tu perfil público, que incluye tu nombre o identificador de usuario, tu rango de edad y país/idioma, tu lista de amigos y cualquier información que compartas con ellos. La información que recopilan estas aplicaciones, sitios web o servicios integrados está sujeta a sus propias condiciones y políticas.

Obtén más información sobre cómo puedes controlar la información personal que tú u otras personas compartís con estas aplicaciones y sitios web.

Compartir información dentro de las empresas de Facebook.

Compartimos la información que tenemos sobre ti dentro del grupo de empresas que pertenecen a Facebook.
Obtén más información acerca de nuestras empresas.

Nuevo propietario.

Si cambian la propiedad o el control de la totalidad o de parte de nuestros servicios o de sus activos, podemos transferir tu información al nuevo propietario.

Compartir información con socios externos y clientes

Colaboramos con empresas que nos ayudan a prestar nuestros servicios y a mejorarlos, o que utilizan productos publicitarios o relacionados; gracias a ellas, podemos gestionar nuestras empresas y proporcionar servicios gratuitos a personas de todo el mundo.

Estos son los tipos de colaboradores externos con los que podemos compartir información sobre ti:

Servicios de publicidad, medición y análisis (solo información que no permita la identificación personal).

Queremos que la publicidad que encuentres en Facebook sea tan relevante e interesante como el resto de la información que veas en nuestros servicios. Con este objetivo, utilizamos toda la información que tenemos acerca de ti para mostrarte anuncios relevantes. No compartimos información mediante la que se te pueda identificar (esto es, información como tu nombre o tu dirección de correo electrónico que pueda utilizarse para contactar contigo o para identificarte) con socios de publicidad, medición y análisis, a menos que nos des permiso para ello. Podemos proporcionar a estos socios información acerca del alcance y la eficacia de su publicidad sin incluir información que te identifique, o podemos concentrar la información de tal forma que no se te pueda identificar. Por ejemplo, podemos informar a un anunciante acerca del rendimiento de sus anuncios o del número de personas que han visto sus anuncios o que han instalado una aplicación tras ver un anuncio; también podemos proporcionarles a estos socios información demográfica que no les permita identificarte (por ejemplo, "mujer de 25 años residente en Madrid a la que le gusta la ingeniería de software"), para ayudarles a conocer a su público o a sus clientes, pero solo una vez que el anunciante haya aceptado cumplir nuestras normas para anunciantes.

Consulta tus preferencias de publicidad para entender por qué ves un determinado anuncio en Facebook. Puedes ajustar tus preferencias de anuncios si quieres controlar y administrar la publicidad que ves en Facebook.

Proveedores generales, proveedores de servicios y otros socios.

Transferimos información a proveedores generales, proveedores de servicios y otros socios de todo el mundo que nos ayudan a mantener nuestro negocio prestando servicios de infraestructura técnica, analizando el uso que se hace de nuestros servicios, midiendo la eficacia de los anuncios y servicios, ofreciendo atención al cliente, facilitando los pagos o realizando investigaciones académicas y encuestas. Estos socios deben cumplir estrictas obligaciones de confidencialidad que se ajustan a esta política de datos y a los acuerdos que suscribimos con ellos.

¿Cómo puedo administrar o eliminar información sobre mí?

Puedes administrar el contenido y la información que compartes al usar Facebook mediante el registro de actividad. También puedes descargar información asociada a tu cuenta de Facebook con nuestra herramienta Descarga tu información.

Almacenamos los datos durante el tiempo necesario para facilitarte productos y servicios, a ti y otros usuarios, incluidos los descritos anteriormente. La información asociada a tu cuenta se conservará hasta que la cuenta se elimine, a menos que ya no necesitemos los datos para ofrecer productos y servicios.

Puedes eliminar tu cuenta en cualquier momento. Cuando elimines tu cuenta, eliminaremos lo que hayas publicado, como tus fotos y actualizaciones de estado. Si no quieres eliminar tu cuenta, sino dejar de utilizar temporalmente Facebook, puedes desactivarla. Para obtener más información sobre cómo desactivar o eliminar tu cuenta, haz clic aquí. Recuerda que la información que otras personas hayan compartido sobre ti no forma parte de tu cuenta, por lo que no se eliminará cuando elimines la cuenta.

¿Cómo respondemos a requerimientos legales o evitamos que se produzcan lesiones?

Podemos acceder a tu información, conservarla y compartirla en respuesta a un requerimiento legal (como una orden de registro, orden judicial o citación) si creemos de buena fe que la ley así lo exige. Esto puede incluir la respuesta a requerimientos legales de jurisdicciones ajenas a los Estados Unidos cuando creamos de buena fe que la ley de esa jurisdicción exige dicha respuesta, que afecta a los usuarios en dicha jurisdicción y que resulta coherente con estándares reconocidos internacionalmente. También podemos acceder, conservar y compartir información cuando creamos de buena fe que es necesario: detectar, evitar y responder al fraude y a otras actividades ilegales; protegernos a nosotros mismos, a ti y a otros usuarios, incluso como parte de investigaciones; o evitar que se produzcan lesiones físicas inminentes o mortales. Por ejemplo, podemos proporcionar información a socios externos acerca de la fiabilidad de tu cuenta con el fin de prevenir el fraude y un uso incorrecto dentro y fuera de nuestros servicios. Es posible que consultemos, procesemos o conservemos la información que recibamos sobre ti (incluida información sobre transacciones financieras relativa a compras realizadas con Facebook) durante un período prolongado de tiempo cuando esté sujeta a una solicitud u obligación judicial, una investigación gubernamental o investigaciones relacionadas con posibles infracciones de nuestras políticas o condiciones, o bien para evitar daños. También conservamos información sobre las cuentas que se han desactivado al incumplir nuestras condiciones y guardamos sus datos durante un año como mínimo para así evitar que se repitan las conductas abusivas o las infracciones de nuestras condiciones.

¿Cómo funcionan nuestros servicios globales?

Facebook, Inc. cumple el marco Safe Harbor entre Estados Unidos y la Unión Europea y entre Estados Unidos y Suiza con relación a la recopilación, el uso y la retención de datos pertenecientes a la Unión Europea y Suiza, según lo dispuesto por el Departamento de Comercio de Estados Unidos. Para consultar nuestra certificación, visita el sitio web de Safe Harbor. Como parte de nuestra participación en el programa Safe Harbor, resolveremos todos los posibles conflictos que puedan surgir en relación con nuestras políticas y prácticas a través de TRUSTe. Puedes contactar con TRUSTe a través de su sitio web.

Facebook puede compartir información por vías internas en el seno de su grupo de empresas o con terceros con los fines que se describen en esta política. La información recopilada dentro del Espacio Económico Europeo ("EEE") puede, por ejemplo, transferirse a países de fuera del EEE a los efectos descritos en esta política.

¿Cómo te notificaremos los cambios que se produzcan en esta política?

Te avisaremos antes de realizar cambios importantes en esta política y te daremos la oportunidad de revisar y hacer comentarios sobre la política revisada antes de que continúes utilizando nuestros servicios.

Cómo hacer llegar tus dudas a Facebook

Para obtener más información sobre la privacidad en Facebook, consulta Aspectos básicos de la privacidad. Si tienes preguntas acerca de esta política, puedes ponerte en contacto con nosotros utilizando la siguiente información:

Si vives en Estados Unidos o en Canadá...

Ponte en contacto con Facebook, Inc. A través de internet o por correo postal en la dirección:

Facebook, Inc.
1601 Willow Road
Menlo Park, CA 94025

Si vives en otro país...

El controlador de datos responsable de tu información es Facebook Ireland Ltd., con quien te puedes poner en contacto a través de internet o por correo postal en la dirección:

Facebook Ireland Ltd.
4 Grand Canal Square
Grand Canal Harbour
Dublin 2 Ireland

Fecha de la última revisión: 30 de enero de 2015

Capítulo 10

Referencias

[1] - http://www.trecebits.com/2015/03/24/nuevo-mapa-de-las-redes-sociales-2015/
http://franbarquilla.com/el-estado-de-internet-y-las-redes-sociales-en-2015-en-espana-y-en-todo-el-mundo/
http://www.multiplicalia.com/las-redes-sociales-mas-usadas/
Ultimo acceso 21/09/2015.

[2] – http://www.iabspain.net/wp-content/uploads/downloads/2015/01/Estudio_Anual_Redes_Sociales_2015.pdf
Ultimo acceso 21/09/2015.

[3] - http://es.wikipedia.org/wiki/Red_social
Ultimo acceso 21/09/2015.

[4]-
http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=12&id_tema=163
Ultimo acceso 21/09/2015

[5] - http://www.erroreshistoricos.com/curiosidades-historicas/888-la-teoria-de-los-seis-grados-de-separacion.html
Ultimo acceso 21/09/2015

[6] - http://www.informatica-hoy.com.ar/redes-sociales/La-historia-de-las-redes-sociales.php
Ultimo acceso 21/09/2015

[7] - http://www.informatica-hoy.com.ar/internet/Que-es-Web-2.0.php
http://es.wikipedia.org/wiki/Web_2.0
Ultimo acceso 21/09/2015

[8] - http://www.genbeta.com/redes-sociales-y-comunidades/google-se-desintegra-photos-y-streams-quedan-bajo-el-mando-de-bradley-horowitz

Ultimo acceso 21/09/2015

[9] - http://www.economiza.com/2015/01/15/tuenti-cambia-de-ceo-y-promete-mejorar-resultados-en-2015/
Ultimo acceso 21/09/2015

[10] - http://www.jambitz.com/10-redes-sociales-para-aficiones-particulares/
Ultimo acceso 13/05/2015 – NO DISPONIBLE

[11] - http://es.slideshare.net/OscarIvanRoaMarin/redes-sociales-17528622
Ultimo acceso 21/09/2015

[12] - http://queaprendemoshoy.com/que-es-la-web-3-0/
Ultimo acceso 21/09/2015

[13] - http://www.obs-edu.com/noticias/estudio-obs/espana-aumenta-el-numero-de-usuarios-activos-en-redes-sociales-en-2014-y-llega-los-17-millones/
http://www.elmundo.es/blogs/elmundo/el-gadgetoblog/2015/03/31/desmontando-google.html
Ultimo acceso 21/09/2015

[14] - http://goandweb.com/cuantos-usuarios-hay-en-activo-en-las-redes-sociales-2014/
http://hipertextual.com/2015/02/estado-de-las-redes-sociales-2015
Ultimo acceso 21/09/2015

[15] - http://recursostic.educacion.es/observatorio/web/en/internet/web-20/1043-redes-sociales?start=3
http://www.pabloburgueno.com/2009/03/clasificacion-de-redes-sociales/
Ultimo acceso 21/09/2015

[16] – http://queaprendemoshoy.com/cual-es-el-futuro-de-las-redes-sociales/
Ultimo acceso 21/09/2015

[17] -
http://es.wikipedia.org/wiki/Medios_sociales#Medios_sociales_y_los_Medios_de_comunicaci.C3.B3n_de_masas
Ultimo acceso 21/09/2015

[18] - http://www.brandchats.com/china-y-sus-7-redes-sociales-prohibidas/
Ultimo acceso 03/06/2015 – NO DISPONIBLE

[19] -
http://www.elmundo.es/internacional/2014/10/01/542af3e9268e3e7e3b8b456f.html
Ultimo acceso 21/09/2015

[20] - http://www.vanguardia.com/historico/65662-investigan-trata-de-blancas-en-la-red-facebook
http://www.elcolombiano.com/redes-sociales-amplifican-amenazas-del-terrorismo-cia-LG1495872
http://www.rtve.es/noticias/20140912/yihadismo-navega-redes-sociales/1009760.shtml
Ultimo acceso 21/09/2015

[21] - http://recursostic.educacion.es/observatorio/web/ca/internet/web-20/1043-redes-sociales?start=5
Ultimo acceso 21/09/2015

[22] - http://vlcnoticias.com/una-manifestacion-convocada-por-las-redes-sociales-provoca-danos-en-varios-edificios/
Ultimo acceso 21/09/2015

[23] - http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-105-4.PDF
http://nosomosdelito.net/article/2015/03/03/recta-final-para-la-aprobacion-de-las-leyes-mordaza

Ultimo acceso 21/09/2015

[24] - http://www.marketingdirecto.com/actualidad/social-media-marketing/las-redes-sociales-dominan-la-difusion-informativa/
Ultimo acceso 21/09/2015

[25] - http://mglobalmarketing.es/blog/el-marketing-3-0-segun-philip-kotler-y-sus-10-mandamientos/
Ultimo acceso 21/05/2015 – NO DISPONIBLE

[26] - http://www.obs-edu.com/noticias/estudio-obs/espana-aumenta-el-numero-de-usuarios-activos-en-redes-sociales-en-2014-y-llega-los-17-millones/
Ultimo acceso 21/09/2015

[27] - http://www.abc.es/hemeroteca/historico-06-02-2003/abc/Madrid/sanchez-romero-cometio-una-infraccion-grave-al-no-proteger-datos-personales_160299.html
http://cincodias.com/cincodias/2002/07/04/economia/1025762186_850215.html
Ultimo acceso 21/09/2015

[28] - http://www.puromarketing.com/53/17969/responsables-recursos-humanos-utiliza-redes-sociales-para-encontrar.html
Ultimo acceso 21/09/2015

[29] - http://www.lne.es/sociedad-cultura/2015/02/10/despedida-twitter/1711127.html
Ultimo acceso 21/09/2015

[30]-
http://es.wikisource.org/wiki/Declaraci%C3%B3n_Universal_de_los_Derechos_Humanos
Ultimo acceso 21/09/2015

[31] - http://es.wikipedia.org/wiki/Privacidad_en_Internet
Ultimo acceso 21/09/2015

[32] - http://www.enfolang.com/internacional/redes-sociales/privacidad-redes-sociales.html
Ultimo acceso 21/09/2015

[33] - http://www.acnur.org/t3/fileadmin/scripts/doc.php?file=t3/fileadmin/Documentos/BDL/2001/0015
Ultimo acceso 21/09/2015

[34] - http://www.securityartwork.es/2012/09/07/puerto-seguro-vs-lopd/
Ultimo acceso 21/09/2015

[35] - https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229
Ultimo acceso 21/09/2015

[36] - http://www.boe.es/boe/dias/1985/11/15/pdfs/A36000-36004.pdf
Ultimo acceso 21/09/2015

[37] - http://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678
Ultimo acceso 21/09/2015

[38] - http://www.boe.es/buscar/doc.php?id=DOUE-L-2001-81549
Ultimo acceso 21/09/2015

[39] - http://www.boe.es/buscar/act.php?id=BOE-A-1982-11196
Ultimo acceso 21/09/2015

[40] - http://derecho.isipedia.com/cuarto/derecho-del-consumo/10-los-contratos-a-distancia

http://noticias.juridicas.com/base_datos/Admin/rdleg1-2007.l1t1.html
http://www.boe.es/buscar/act.php?id=BOE-A-2007-20555
Ultimo acceso 21/09/2015

[41] - http://www.boe.es/buscar/act.php?id=BOE-A-1996-8930
https://www.boe.es/boe/dias/2014/11/05/pdfs/BOE-A-2014-11404.pdf
Ultimo acceso 21/09/2015

[42] -http://es.wikipedia.org/wiki/Tratado_de_la_OMPI_sobre_Derecho_de_Autor
Último acceso 21/09/2015

[43] - http://actualidad.rt.com/actualidad/view/57367-facebook-se-usa-secuestro-trafico-menores-indonesia
Último acceso 21/09/2015

[44] - http://www.europapress.es/portaltic/socialmedia/noticia-mark-zuckerberg-facebook-censura-libertad-expresion-20150116170203.html
Último acceso 21/09/2015

[45] - http://es.wikipedia.org/wiki/Derecho_al_olvido
http://boe.es/legislacion/codigos/codigo.php?id=94&modo=1&nota=0
http://politica.elpais.com/politica/2015/01/23/actualidad/1422015745_590889.html
http://sociedad.elpais.com/sociedad/2014/05/12/actualidad/1399921965_465484.html
Último acceso 21/09/2015

[46] -
http://www.lavanguardia.com/tecnologia/internet/20140530/54409461842/google-formulario-derecho-olvido.html
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=es
Último acceso 21/09/2015

[47] - http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t11.html

Último acceso 21/09/2015

[48] – http://www.delitosinformaticos.com/10/2013/noticias/calumnias-e-injurias-en-internet
http://www.legaltoday.com/practica-juridica/civil/nuevas_tecnologias/condena-a-dos-jovenes-toledanas-por-injuriar-en-facebook-y-tuenti
http://politica.elpais.com/politica/2014/05/07/actualidad/1399479799_383719.html
http://www.diaridetarragona.com/noticia.php?id=40258
http://www.delitosinformaticos.com/10/2013/noticias/calumnias-e-injurias-en-internet
Último acceso 21/09/2015

[49] - http://www.elmundo.es/deportes/2015/04/02/551d17ffca4741c2358b458a.html
http://www.20minutos.es/noticia/2237647/0/pp-masnou/disculpas-amenaza/artur-mas/
http://www.huffingtonpost.es/2014/11/07/jonathan-cabeza-infante_n_6119516.html
http://www.abc.es/madrid/20140429/abci-ganas-tengo-darte-tiro-201404282127.html
http://cadenaser.com/emisora/2015/03/30/radio_valencia/1427719606_402786.html
http://www.eldiario.es/politica/PP-amenazas-concejal-Azuqueca-Guadalajara_0_359764424.html
Último acceso 21/09/2015

[50]- http://www.publico.es/politica/ts-confirma-condena-15-jovenes.html
http://fuenlabradanoticias.com/condenada-por-espiar-el-movil-de-su-marido/
Último acceso 07/06/2015

[51] -
http://politica.elpais.com/politica/2015/05/22/actualidad/1432324829_320181.html
Último acceso 07/06/2015

[52] - http://www.quenoteladen.com/que_es_grooming.php
Último acceso 07/06/2015 – NO DISPONIBLE

[53]- **http://politica.elpais.com/politica/2015/05/26/actualidad/1432623198_485097.html**

Último acceso 21/09/2015

[54] - http://www.policia.es/org_central/judicial/udef/alertas/20110404_1.html

Último acceso 21/09/2015

[55] - http://www.genbeta.com/seguridad/atentos-a-una-nueva-forma-de-phishing-el-tabnabbing

Último acceso 21/09/2015

[56] - https://jacarballar.wordpress.com/2012/10/30/que-es-el-spam-de-twitter-y-su-relacion-con-el-secuestro-de-cuentas/

Último acceso 21/09/2015

[57] - http://www.mujeresycia.com/?x=nota/45764/1/anorexia-y-bulimia-perfiles-de-twitter-y-facebook-las-promueven

Último acceso 21/09/2015

[58] - http://ccaa.elpais.com/ccaa/2015/03/26/valencia/1427365189_272397.html

Último acceso 21/09/2015

[59] - http://www.diariopopular.com.ar/notas/205107-las-redes-sociales-campos-fertiles-la-pedofilia

http://www.elmanana.com/pgjeminvestigavideodepresuntopedofiloenredessociales-2806875.html

Último acceso 21/09/2015

[60] - http://www.20minutos.es/noticia/2428742/0/facebook-reconoce/haber-rastreado-error/ususarios-ajenos/

http://www.dealerworld.es/redes-sociales/detenida-una-banda-que-buscaba-en-facebook-informacion-para-sus-robos

http://tecnologia.elpais.com/tecnologia/2015/08/19/actualidad/1439982485_545659.html
Último acceso 21/09/2015

[61] - http://www.que.es/tecnologia/201405270800-adiccion-redes-sociales-afecta-felicidad.html
http://www.cromo.com.uy/2014/11/por-que-las-redes-sociales-generan-adiccion/
Último acceso 07/06/2015 – NO DISPONIBLE

[62] - http://www.exclusive-networks.es/las-tecnicas-de-robo-de-datos-y-los-ataques-por-inyeccion-sql-los-preferidos-por-los-hackers-segun-imperva/
http://mundocontact.com/los-10-tipos-de-ataques-ddos-mas-comunes/
Último acceso 21/09/2015

[63] - http://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL
Último acceso 21/09/2015

[64] - http://economia.elpais.com/economia/2015/01/05/actualidad/1420480399_157936.html
Último acceso 21/09/2015

[65] - http://www.expansion.com/2011/01/05/juridico/1294267832.html
Último acceso 21/09/2015

[66] - http://www.enriquedans.com/2013/02/sobre-ninos-edades-minimas-y-redes-sociales.html
Último acceso 21/09/2015

[67] - http://verne.elpais.com/verne/2015/03/11/articulo/1426096766_908610.html
Último acceso 21/09/2015

[68] - http://www.europapress.es/nacional/noticia-proteccion-datos-anima-no-aceptar-mas-opciones-defecto-privacidad-moviles-redes-sociales-20140128130255.html
Último acceso 21/09/2015

[69] - https://www.fayerwayer.com/2014/05/facebook-incrementa-la-privacidad-por-defecto-en-publicaciones-de-usuarios-nuevos/
Último acceso 21/09/2015
[70] - http://www.20minutos.es/noticia/2429635/0/campana-spam/email-correos/estafa-usuarios/
Último acceso 21/09/2015

[71] - http://www.redeszone.net/2015/02/15/cerrados-sitios-web-falsos-que-simulaban-ser-de-paypal/
Último acceso 21/09/2015

[72]-http://www.pcworld.es/seguridad/un-estudio-espanol-descubre-60-vulnerabilidades-en-22-modelos-de-routers
http://www.abc.es/tecnologia/moviles-telefonia/20140801/abci-seguridad-fallos-smartphones-201408011530.html
Último acceso 21/09/2015

[73] - http://www.borrardatosinternet.com/ono-sancionada-por-ceder-datos-de-clientes-a-guias-y-buscadores-de-internet/
http://www.borrardatosinternet.com/las-electricas-entre-las-companias-mas-sancionadas-por-la-aepd/
https://www.samuelparra.com/2014/02/14/groupon-sancionada-por-no-informar-almacenaba-datos-tarjetas-credito-cvv-clientes/
Último acceso 21/09/2015

[74] - http://noticias.juridicas.com/actualidad/jurisprudencia/5411-las-direcciones-ip-de-los-usuarios-de-internet-deben-ser-consideradas-como-datos-personales-y-por-tanto-estan-protegidos-por-la-lopd/

Último acceso 21/09/2015

[75] - http://tecnologia.elpais.com/tecnologia/2015/08/22/actualidad/1440226457_464503.html
Último acceso 21/09/2015

[76] http://www.informationweek.com.mx/analysis/seguridad-primordial-para-la-confianza-en-las-marcas-digitales/
Último acceso 19/09/2015

[A] -
https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.pdf
Último acceso 19/09/2015

Otra documentación consultada:

<<Guía sobre adolescencia y sexting: qué es y cómo prevenirlo>>. INTECO. Febrero 2011. Pérez San José, Pablo y otros.

<<Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online>>. INTECO. Febrero 2009.

<<IV Estudio Redes Sociales de IAB Spain>>. IOAB Spain. Enero 2015.

<< **Six Degrees: The Science of a Connected Age>>.** Watts, Duncan J**.** 2004.

<< Monográfico Redes sociales – Definición de redes sociales>>. Observatorio Tecnológico de España. Abril 2012. Ponce, Isabel.

<< Monográfico Redes sociales – Redes sociales educativas>>. Observatorio Tecnológico de España. Abril 2012. Ponce, Isabel.

<<El tratamiento del llamado delito informático en el proyecto de ley orgánica de código penal: reflexiones y propuestas de la CLI (Comisión de Libertades e Informática)>>. Informática y derecho, 1996, n.12, p. 1149-1162. Fernández Calvo, Rafael.

<<The impact of social networking on the IT audit universe>>. ISACA. Gibbs, Nelson.

<<Social Media: Bussines benefits and security, governance and assurance persepectives>>. ISACA. 2010. Rico, Salomon

<<3 Step Guide to safe Social Media>>. ISACA.

<<Guía de seguridad de datos>>. AEPD. 2012.